Acta Technica 62 (2017), No. 7A, 951–964

Defense situation assessment of network warfare information security based on dynamic bayesian network

Rong Li[1], Bing Tian[1], Li Yan[1], Yansheng Qu[1]

Abstract. With development of global informatization, increasingly rampant information security event has caused wide attention of people to information security problem. However, current information security technology based on traditional defense technology is hard to deal with it. Therefore, experts of information security start to focus on information security technology research based on active defense thought. At present, research on information security defense technology mainly focuses on active defense for information security relevant to security situation evaluation and security threat prediction. From the perspective of technology, based on Bayes Model, research has been implemented to security situation evaluation method in information security field and attack route prediction method. Put forward a kind of evaluation method for evaluating overall system security and vulnerabilities severity degree, which can effectively evaluate overall system security and vulnerabilities severity degree.; firstly, put forward a kind of Cause Result Detection Algorithm (CRDA) to confirm causal relationship; secondly, provide Bayes Attach Diagram and provide generation algorithm BAGA of BAG according to system structure of attack model; finally, it is proved that the method can effectively solve error calculation problem of node confidence coefficient by experiment to accurately predict transmission route of network threat.

Key words. Bayes, Network security, Defense, Evaluation, Intrusion detectio.

1. Introduction

This Paper has put forward network security situation evaluation model based on Bayes Network because traditional network security evaluation model cannot perceive network security situation. The situation evaluation model is divided into 3 layer structure according to function. Node of Bayes Network shall be divided into situation node and event node according to function; take network and information acquisition of host tool as evidence of event node by network reasoning process to update situation node probability and to influence probability of event node in re-

[1] State Grid Shandong Electric Power Corporation, Jinan 250021, China

turn, so as to confirm network security situation. Network space attack information security defense situation is to establish dynamic Bayes Network to evaluate network space attack situation for evaluation aiming at situation evaluation concept put forward by network center station, which can feed back information to deciders quickly, effectively and visually and provide a kind of efficient informatization assisting decision and support, so that information security defense system can take effect better and can better promote resistance of information system for development of the new resistance mode. Concept of information security defense situation comes from Information Assurance (IA) put forward by American Army, which mainly aims at connect sensor in war field network space, command decider and war unit into a whole to share situation perception information. Based on information integration technology, instruction decision technology and GIG, simulating comprehensive perception of factors relevant to instruction decision in corresponding war field, so as to know and have a command of current information security situation of war fields and implement credit prediction to action taken by enemy recently and war results and to implement real-time and complete evaluation to war field condition and threat and importance degree and to realize highly dynamic real-time and interactive operation to information security assurance organization command activity, which aims at changing information advantages into fighting capacity. Foreign researches on the field start early and develop rapidly and great achievements have been achieved in research and development of theory and corresponding systems; domestic researches in the field are still in starting stage and research methods are not very specific, which aims at implementing static evaluation to information security defense system of war field network and analysis on unknown threat is not thorough, so that situation evaluation is hard to be dynamic, autonomous and controllable and hard to know influence of unknown and uncertain information on information security situation. Fuzzy Dynamic Bayesian Network (Fuzzy Dynamic Bayesian Network) is a development direction in space situation evaluation field method application. When situation information acquired by sensor is fuzzy and uncertain on time sequence, influence caused by middle information change in the whole war field network system can be perceived and evaluated continuously, which can provide a more active and accurate quantitative analysis and assistant decision means for problem solving for grasping and research and judgment of situation during network space information security defense.

2. Situation evaluation

2.1. Principle of situation evaluation

Characteristics of network war information security defense decide relatively strong timeliness and co-movement of its situation evaluation process; namely, it has realized continuous perception and analysis on security situation of its own network at certain time node and has realized evaluation and warning to future security situation and process includes two parts of situation perception and threat evaluation, which is comprehensive reflection of all situation factors in information security defense and all factors are closely connected and a situation factor usually constrains and influences other factors in defense process; therefore, it shall take dependency, dynamics, uncertainty and continuity among target network situation factors into consideration during dynamic evaluation, so as to analyze its causal association. Therefore, connect all situation factors in information security defense to establish layer relationship and acquire all factors to be considered for threat evaluation by situation perception means; predict potential threat event according to security event probability prediction at known moment and evaluate for monitoring information security defense situation to predict development trend of information security defense.

2.2. Situation evaluation characteristics of network space war information security defense

1) Co-movement. Co-movement means that change of local defense situation or situation factor of its own network directly influences whole evaluation of information security situation of the whole network system and all-layer information activity link or information process in network will lead to condition change of situation factors, which will cause correlation effect and interlocking reaction to defense system of the whole network from the one to the other and from surface to the centre.

2) Completeness. Complete evaluation index system is basis of knowing evaluation object comprehensively, objectively and accurately and threat situation condition of network space can be reflected comprehensively by establishing a set of scientific, reasonable and comprehensive defense situation evaluation index system of network space information security and by selecting complete evaluation indexes.

3) Operability. Evaluation method established can convert situation factors that are hard be to researched by quantitative method into data that can be measured, calculated and compared and can ensure feasibility of data extraction acquisition in evaluation process, so that the whole process of evaluation will be transparent and reliable and easy to be operated and input data required for evaluation shall be easy to be acquired.

3. Dynamic Bayes Network inference and fuzzy comprehensive evaluation

3.1. Cause of selecting Dynamic Bayes Network

Dynamic Bayes Network (DBN) is time sequence of Bayes Network (BN), which has function characteristics of Static Bayes Network and has embodied influence of sample data on network structure more accurately in time domain and the method is applicable to influence evaluation of situation factor change in information security defense situation of network space war on the whole defense system. Integrate time sequence casual association at adjacent time section with casual association of the same time section and implement dynamic analysis by quantization inference and DBN can be simply defined as $(B_0, B_{\rightarrow})$; B_0 is BN at T_0 (time section of initial condition) and prior probability P(X_0) of hidden node and observation point can be got from BN structure and is diagram formed by BN at all time sections.

DBN has the functions of integrating new knowledge and expressing, interfering and learning matters and has relatively favorable effect during modeling analysis for uncertain problems of radon process nature and network structure of DBN is shown as Fig.1:

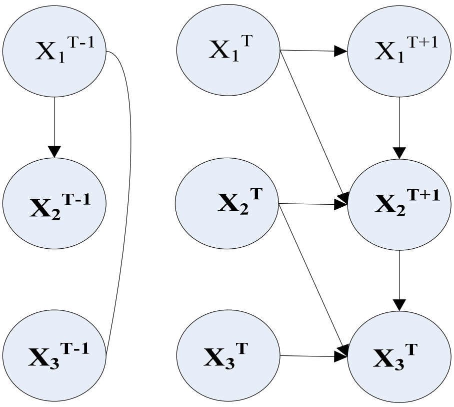

Fig. 1. Dynamic Bayes Network structure

3.2. Inference algorithm of DBN

DBN inference algorithm is inferred from Bayes Formula of Formula (1):

$$p(x\,|y) = \frac{p(yx)}{p(y)} = \frac{p(yx)}{\sum\limits_{x} p(yx)\,.} \tag{1}$$

Its inference process is the same with essence of Static Bayes Network. For disperse Static Bayes Network with n hidden nodes and m observation nodes, according to condition independence characteristics, its inference principle can be reflected into math process of formula (2):

$$\begin{gathered} p(x_1, x_2, ..., x_n\,|y1, y2, ..., y_m\,) = \\ \frac{\prod\limits_{j} p(y_j\,|p_a(Y_j))\prod\limits_{i} p(x_i\,|p_a(X_i))}{\sum\limits_{x_1,x_2,...,x_n}\prod\limits_{j} p\,(yj\,|p_a(Yj)\,)\prod\limits_{i} p\,(x_i\,|p_a(X_i)\,)} \\ i \in [1,n]\,, j \in [1,m]\ . \end{gathered} \tag{2}$$

In above formula, x_i is a condition value $X_i$and $p_a(Y_j)$ shows parent node collection of Y_j.

(3):When hidden nodes and observable nodes are few or coupling of nodes is relatively strong; network structure layers are relatively few and time sections to be considered are few in network, all time sections of DBN can be deemed as a Static Bayes Network; when nodes increase or node coupling performance increases, DBN formed by time sections of the number of T in time domain can be obtained, of which inference process can be reflected in formula (3):

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

$$\sum_{y_{11}y_{12}\cdots y_{Tm}} \frac{\prod\limits_{i,j} p(y_{ij}\,|p_a(Y_{ij}))\prod\limits_{i,k} p(x_{ik}\,\Bigg|\,p_a(X_{ik}))\prod\limits_{i,j} p(Y_{ijo}=y_{ijo})}{\sum\limits_{x_{11},x_{21},...,x_{T1}\cdots x_{Tn}}\prod\limits_{i,j} p\left(y_{ij}\,|p_a(Y_{ij})\right)\prod\limits_{i,k} p\left(x_{ik}\,|p_a(X_{ik})\right)}$$

$$i \in [1,T]\,, j \in [1,m]\,, K \in [1,n] \tag{3}$$

In foresaid formula, x_{ij} is a condition value of X_{ij}; i is time section ; j represents hidden nodes ; y_{ij} is value of observation variance Y_{ij}; $p_a(Y_{ij})$ is parent node collection y_{ij}; Y_{ijo} is observation condition of observation node j in the time section i and $p(Y_{ijo} = y_{ijo})$ represents that continuous observation value of Y_{ij} belongs to membership of condition y_{ij}.

3.3. Cause of selecting fuzzy comprehensive evaluation method

Fuzzy comprehensive evaluation analyzes complex fuzzy system by applying fuzzy conversion principle, which is used to multi-attribute decision-making problems and make comprehensive decision to problems by analysis and fuzzy judgment of quantization and quantification on considerable complex influence factors. Evaluation index set of information security defense situation of network space can be taken as a multi-index evaluation problem and index factor to be established shall be analyzed comprehensively in multi-layer and multi-factor ways and all-layer situation index of evaluation network established and complexity degree is high; therefore, it adapts to such method.

4. Evaluation model establishment

4.1. Perception model for information security defense of network space war

Primary task of situation evaluation is to realize evaluation object situation perception and comprehensive perception to important situation factors is formed to establish situation perception model; otherwise, probability for error situation estimation will be increase and successful network space information system model shall be flexible and dynamic, which can realize the whole process [4] for data acquisition, perception, prediction and exploring data further and can form reasonable defense scheme; therefore, defense situation perception of network space information security not only includes from recognition to information, but also includes information integration and situation image of structure planning can be formed by importance degree judgment of objects and events., which includes element extraction, current situation evaluation analysis and future situation prediction relevant to information security environment and its process mainly covers the following aspects: Firstly, under certain environment, extract various factors to be considered for situation evaluation and make preparation for situation inference, so as to analyze and confirm profound cause for events and to provide current situation comprehending or comprehensive evaluation of evaluated object and judge events at known moments, so as to confirm development trend of situation. Situation factors mainly involve information asset, enemy threat and resistance and implement modeling for perception result of defense situation and implement evaluation to security and risk condition of current war network space [5]. Network space defense situation perception model is shown as Fig. 2.

4.2. Situation factor analysis of information security defense for network space war

Situation factors include information security assurance measures, assurance ability for security defense strength and information environment factors, etc., which generally consist of four situation categories: condition monitoring situation, resistance situation, defense situation and emergency situation and all categories consist of different basis factors, as shown in Table 1 and key point of defense can be adjusted mainly during defense by evaluating threat class of its own network and clarify aspects to be improved and completed.

These factors influence interactively and decide war defense threat situation of network space and are data acquired for evaluation [6].

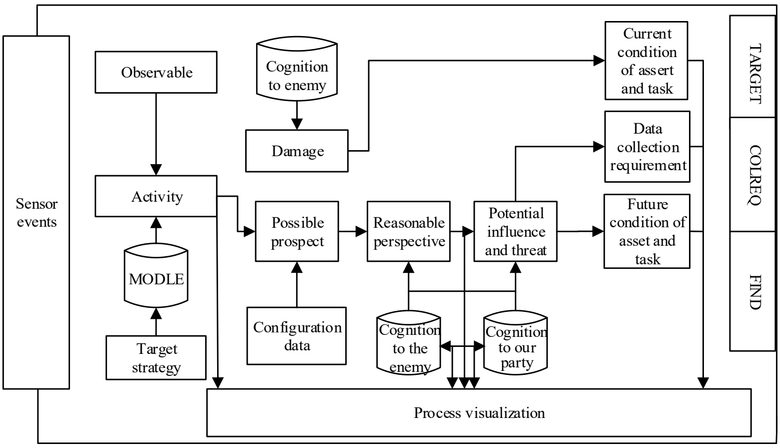

Fig. 2. Perception model for information security defense situation for network space war 4.3 establishment of dynamic bayes evaluation network

Table 1. Factor components for information security defense situation of network space war

		Factor Parameters for Basic Situation						
Situation supervision situation	Network detection	Information acquisition probability	Acquisition delay	Information retrieval rate	Information integration rate	Information distribution rate		
	Network warning	Identification friend or foe probability	Identification friend or foe time	Threat evaluation delay	Pseudo judgment rate			
Resistance situation	Password defense	Password system reliability	Whitened degree password analysis	Password analysis time	Equipment serviceability rate			
	Network counterattack	Network attack frequency and strength	Rate for spreading interference information					
Defense situation	Network tricking	Service refusal occurrence rate	False news attack occurrence rate	utilization attacking occurrence				
	Technology assurance	Intrusion detection accuracy	Network information transmission rate	Network information transmission rate	Maximal network capacity	Average no-fault time	Key equipment fault recovery rate in network	
	Control decision	Organization plan time	detail degree of organization plan	Command coordination stability probability	Assistant decision time	Decision reliability degree		
Emergency situation	Emergency disposal	Disaster evaluation time	Recovery percentage	Data recovery time	Function reconstruction time	Recovery percentage	Complete backup time	Survival rate for emergency condition of key equipment
	Internetwork support	Internetwork backup equipment and system providing service efficiency	Simultaneous thread count of internetwork backup server					

Evaluation to threat of its own network is mainly to complete threat degree evaluation of prevention network by information acquired by situation perception system and main principle is to further quantify comparison result of quantitative characteristics parameter based on comparing relevant condition characteristics quantity change of situation factor and to finally confirm situation class by considering judgment result of all characteristics parameters comprehensively. Establish fuzzy set of situation factor condition by adopting AHP fuzzy comprehensive evaluation method and establish Dynamic Bayes Network model of threat evaluation according to expert knowledge of relevant fields [7], as shown in Fig. 3.

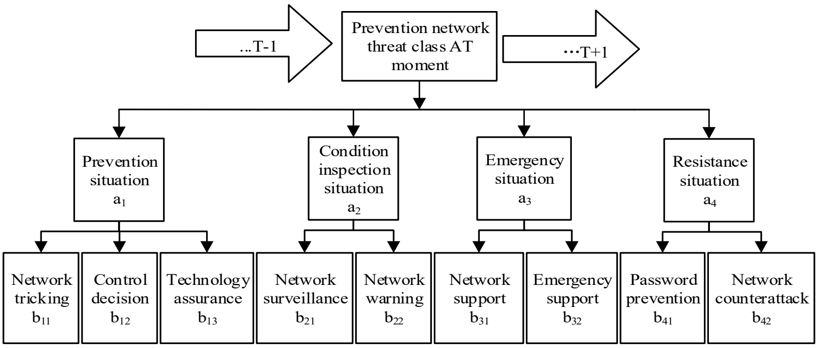

Fig. 3. Dynamic Bayes Network structure figure of network space prevention situation

Classify situation condition according to actual war experience, expert system and key parameter threshold value of different situation factors; after condition of all-class situation factors shall be distinguished [8] according to number obtained by adding of weights after being normalized by the next class factor; for example, nondimensionalization of b$_{21}$ (network inspection) shall be implemented after acquiring probability, delay (minute), information rate (frame/minute), information integration rate (frame/minute) and information distribution rate (frame/minute) according to formula (4).

$$f(x_i) = \frac{x_i}{x_0} = y_i \,. \tag{4}$$

Where, x_i is observation value of various parameters in situation factor b$_{21}$ at a time section; x_0 is number larger than 0; y_i is data after normalization disposal.

Data after normalization shall be added according to weight confirmed by AHP fuzzy comprehensive evaluation as formula (5):

$$\sum_{i=1}^{n} y_i \cdot w(x_i) = z \,. \tag{5}$$

Where, $w(x_i)$ is weight of all factors; z is value corresponding with b$_{21}$; value range $[z_1, z_4]$ of z can be obtained by repeating the process for several times, which is divided into different threshold values $[z_1, z_2]\,, [z_2, z_3]\,, [z_1, z_4]$; corresponding fuzzy condition set $S_{a_{21}} =$ (high investigation degree, middle investigation degree and low investigation degree).

Establish fuzzy set for condition description of all situation factors thereby; S_A and $S_{b_{22}}$ =(high threat, middle threat and weak threat); S_{a_1}, S_{a_2}, $S_{b_{12}}$ and $S_{b_{32}}$=(high stability, middle stability and low stability); S_{a_4}=(strong disaster recovery capability, general disaster recovery capability and weak disaster capability); $S_{b_{41}}$, $S_{b_{42}}$ and $S_{b_{13}}$=(strong, general and weak); S_{a_3} =(high robustness, middle robustness and low robustness).

4.3. Setting of model parameters

Condition probability matrix is a kind of opinion of field experts on casual association of all association nodes in network and is a kind of expert knowledge. Infer threat class [9] of prevention network according to all situation factors condition and its condition probability is shown in Table 2-Table 4 and Table 5 shows condition transfer probability matrix of target network threat class and Table 6 shows probability observation data of situation factors.

Table 2. Condition probability matrix of threat class of prevention network of its own party

A	P(a_1/A) High Middle Low	P(a_2/A) High Middle Low	P(a_3/A) high middle low	P(a_4/A) high middle low
High	0.3 0.4 0.3	0.5 0.3 0.2	0.2 0.5 0.3	0.2 0.5 0.3
Middle	0.6 0.2 0.2	0.4 0.4 0.2	0.5 0.3 0.2	0.3 0.5 0.2
Low	0.1 0.2 0.7	0.2 0.1 0.6	0.1 0.4 0.5	0.1 0.4 0.5

Table 3. Condition probability matrix of situation factors

a_1	P(b_{11}/ a_1) High Middle Low	P(b_{12}/ a_1) High Middle Low	P(b_{13}/ a_1) Strong General Weak	a_2	P(b_{21}/ a_2) High Middle Low	P(b_{22}/ a_2) High Middle Low
High	0.4 0.2 0.4	0.5 0.3 0.2	0.4 0.2 0.4		0.6 0.3 0.1	0.4 0.2 0.4
Middle	0.2 0.4 0.4	0.7 0.2 0.2	0.5 0.3 0.2		0.5 0.3 0.2	0.6 0.2 0.2
Low	0.3 0.3 0.4	0.3 0.2 0.5	0.1 0.3 0.6		0.3 0.3 0.4	0.3 0.4 0.3

Table 4. Condition probability matrix of situation factors

a_3	P(b_{31}/ a_3) High Middle Low	P(b_{32}/ a_3) Strong General Weak	a_4	P(b_{41}/ a_4) Strong General Weak	P(b_{42}/ a_4) Strong General Weak
Strong	0.4 0.2 0.4	0.9 0.1 0.5	Strong	0.5 0.5 0	0.7 0.2 0.1
General	0.7 0.2 0.1	0.2 0.1 0.7	General	0.3 0.4 0.3	0.2 0.3 0.21
Weak	0.1 0.3 0.6	0.2 0.3 0.5	Weak	0 0.3 0.7	0.1 0.5 0.4

Table 5. State transfer probability matrix of network threat class

A(T+1)	High (T+1)	Middle (T+1)	Low (T+1)
A(T)			
High(T)	0.7	0.3	0.2
Middle (T)	0.2	0.5	0.6
Low (T)	0.1	0.2	0.2

Table 6. Probability observation data of situation factor condition

	a_1	a_2	a_3	a_4
T_0	(0.06,0.1,0.84)	(0.1,0.1,0.8)	(0.4,0.2,0.4)	(0.5,0.3,0.2)
T_1	(0.1,0.1,0.8)	(0.2,0.3,0.5)	(0.5,0.2,0.3)	(0.4,0.3,0.3)
T_2	(0.1,0.15,0.75)	(0.3,0.4,0.2)	(0.5,0.3,0.2)	(0.3,0.3,0.4)
T_3	(0.1,0.2,0.7)	(0.4,0.4,0.2)	(0.6,0.3,0.1)	(0.5,0.3,0.2)
T_4	(0.1,0.3,0.6)	(0.5,0.4,0.1)	(0.6,0.2,0.2)	(0.7,0.2,0.1)
T_5	(0.3,0.6,0.1)	(0.6,0.3,0.1)	(0.6,0.3,0.1)	(0.5,0.2,0.3)
T_6	(0.6,0.3,0.1)	(0.7,0.2,0.1)	(0.8,0.1,0.1)	(0.8,0.1,0.1)
T_7	(0.7,0.2,0.1)	(0.8,0.1,0.1)	(0.7,0.2,0.1)	(0,0.2,0.7)
T_8	(0.8,0.1,0.1)	(0.9,0.1,0)	(0.8,0.1,0.1)	(0.8,0,0.2)

5. Actual simulation cases

Based on established evaluation model, this Paper infers by junction tree inference engine of MATLAB BNT tool box. Input all initial data and observation data in Table 2-Table 6 [10].

Information acquired before attack of the opposite party by network space defense strength is very limited and probability distribution that sets initial condition of network threat class as high, middle and low is (0.4, 0.3 and 0.4), which conforms to actual condition assumption and has reflected uncertainty of deciders on situation evaluation grasping by lack of network space situation, so that probability distribution of all conditions in initial setting is close. After entering waiting condition after model initialization, once all nodes in situation information input network has been updated, trigger network reference algorithm, so as to update condition distribution probability of all network nodes [11] and probability distribution of root node condition can be obtained finally.

After finding the opposite party starts attack to network system of us, it is assumed that its attacking moment is continuous, sensor will implement real-time monitoring to network system defense situation and observation value can be set after observing 9 moments continuously according to data obtained at different moments.

1) Situation evaluation based on DBN. Input respectively condition probability distribution of initial network node, network condition transfer probability distri-

bution in DBN evaluation model and implement simulation analysis after acquiring observation data of 9 moments, so as to obtain evaluation analysis result of comprehensive defense situation as shown in Fig.4.

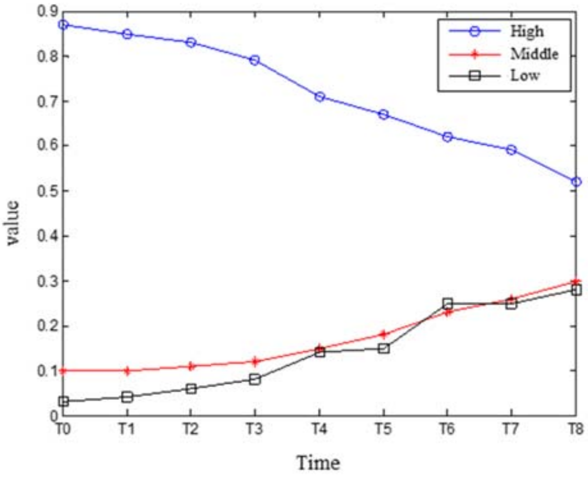

Fig. 4. Result of comprehensive defense situation

2) Establish Statics Bayes Network model and input all data in Table 2-Table 6 and obtain evaluation values as shown in Fig. 5.

Seen from experiment results: with continuous increase of resistance activity frequency, "high" threat class condition probability of prevention network of its own party decreases gradually, while "middle" or "low" condition probability rises gradually and tends to be stable, which shows that it has adapted to resistance method and strength in resistance and information security prevention ability of defense system improves gradually.

Seen from contrast of Fig. 4 and Fig. 5, compared with Statics Bayes Network evaluation, evaluation result of DBN has integrated more feedback relation and observation information among situation factors, which can better reflect objective principle that network war information security changes with time accurately and continuously and is favorable for deciders to better master defense direction and main points and various situation factors will increase with resistance frequency and probability distribution changes gradually and tens to be stable and prevention situation is favorable to tendency development of its own party.

6. Conclusion

It is hard to implement accurate, autonomous and complete controllable evaluation to information security defense situation in network space war; dynamic valuation method based on fuzzy DBN is put forward aiming at such condition so as to implement fuzzy and probability disposal of situation factors in defense system under different time condition and to establish situation perception and situation

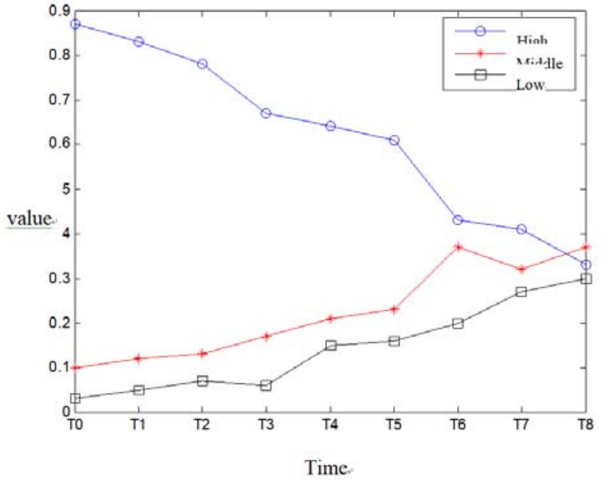

Fig. 5. Simulation result of threat-class fuzzy Static Bayes Network

estimation model Input initial condition probability, condition transfer probability and observation data to model established for simulation experiment and compare simulation result with Static Bayes Network model evaluation result and experiment result shows that evaluation by this methods has integrated feedback relation and observation information among more situation factors and can better reflect objective principle of dynamic change of network space war information security defense situation and can ensure accurate, quick, active and efficient evaluation.

References

[1] J. W. Chan, Y. Y. Zhang, and K. E. Uhrich: *Amphiphilic Macromolecule Self-Assembled Monolayers Suppress Smooth Muscle Cell Proliferation*, Bioconjugate Chemistry, *26* (2015), No. 7, 1359–1369.

[2] Y. J. Zhao, L. Wang, H. J. Wang, and C. J. Liu: *Minimum Rate Sampling and Spectrum Blind Reconstruction in Random Equivalent Sampling.* Circuits Systems and Signal Processing, *34* (2015), No. 8, 2667–2680.

[3] S. L. Fernandes, V. P. Gurupur, N. R. Sunder, N. Arunkumar, S. Kadry: *A novel nonintrusive decision support approach for heart rate measurement*, (2017) Pattern Recognition Letters. https://doi.org/10.1016/j.patrec.2017.07.002

[4] N. Arunkumar, K. Ramkumar, V. Venkatraman, E. Abdulhay, S. L. Fernandes, S. Kadry, S. Segal: *Classification of focal and non focal EEG using entropies.* Pattern Recognition Letters, *94* (2017), 112–117.

[5] W. S. Pan, S. Z. Chen, Z. Y. Feng: *Investigating the Collaborative Intention and Semantic Structure among Co-occurring Tags using Graph Theory.* International Enterprise Distributed Object Computing Conference, IEEE, Beijing, (2012), 190-195.

[6] Y. Y. Zhang, Q. Li, W. J. Welsh, P. V. Moghe, and K. E. Uhrich: *Micellar and Structural Stability of Nanoscale Amphiphilic Polymers: Implications for Anti-atherosclerotic Bioactivity*, Biomaterials, *84* (2016), 230–240.

[7] L. R. Stephygraph, N. Arunkumar, V. Venkatraman: *Wireless mobile robot control through human machine interface using brain signals*, 2015 International Confer-

ence on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials, ICSTM 2015 - Proceedings, (2015), art. No. 7225484, 596–603.

[8] N. Arunkumar, V. S. Balaji, S. Ramesh, S. Natarajan, V. R. Likhita, S. Sundari: *Automatic detection of epileptic seizures using independent component analysis algorithm*, IEEE-International Conference on Advances in Engineering, Science and Management, ICAESM-2012, (2012), art. No. 6215903, 542–544.

[9] Y. Du, Y. Z. Chen, Y. Y. Zhuang, C. Zhu, F. J. Tang, J. Huang: *Probing Nanostrain via a Mechanically Designed Optical Fiber Interferometer.* IEEE Photonics Technology Letters, *29* (2017), 1348–1351.

[10] W. S. Pan, S. Z. Chen, Z. Y. Feng: *Automatic Clustering of Social Tag using Community Detection.* Applied Mathematics & Information Sciences, *7* (2013), No. 2, 675–681.

[11] Y. Y. Zhang, E. Mintzer, and K. E. Uhrich: *Synthesis and Characterization of PEGylated Bolaamphiphiles with Enhanced Retention in Liposomes*, Journal of Colloid and Interface Science, *482* (2016), 19–26.

[12] N. Arunkumar, K. M. Mohamed Sirajudeen: *ApproximateEntropy based ayurvedic pulse diagnosis for diabetics - A case study*,TISC 2011 - Proceedings of the 3rd International Conference on Trendz in Information Sciences and Computing, (2011), art. No. 6169099, 133–135.

Received May 7, 2017