Information Security Defense Situation Assessment of Network Warfare Based on Dynamic Bayesian Network

Hui Baofeng, Jia Guoqing, Chen Shanji

Qinghai University for Nationalities, Xining Qinghai, China

Keywords: Bayes, network security, defense, evaluation, intrusion detection

Abstract: With the 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. This paper puts 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, it puts forward a kind of Cause Result Detection Algorithm (CRDA) to confirm causal relationship; secondly, it provides 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.

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 return, 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. 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

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.

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 T0 (time section of initial condition) and prior probability P(X0) 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:

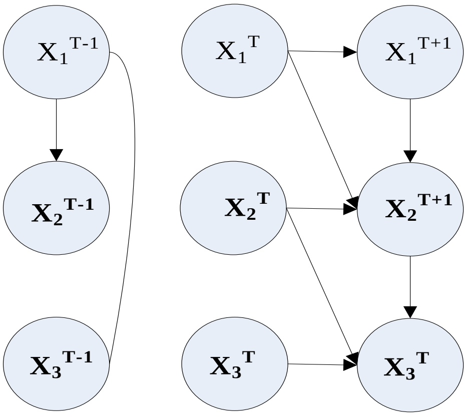

Fig.1. Dynamic Bayes Network structure

3.2 Inference algorithm of DBN

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

$$p(x|y) = \frac{p(yx)}{p(y)} = \frac{p(yx)}{\sum_x p(yx)} \qquad (1)$$

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):

$$p(x_1, x_2, ..., x_n \left| y1, y2, ..., y_m \right.) = \frac{\prod_j p(y_j \left| p_a(Y_j) \right.) \prod_i p(x_i \left| p_a(X_i) \right.)}{\sum_{x_1, x_2, ..., x_n} \prod_j p\left(yj \left| p_a(Yj) \right.\right) \prod_i p\left(x_i \left| p_a(X_i) \right.\right)}$$

$$i \in [1, n], j \in [1, m] \qquad (2)$$

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):

$$p(x_{11}, ..., x_{1n}, ..., x_{T1}, ..., x_{Tn} \left| Y_{11o}, Y_{12o}, ..., Y_{1mo}, ..., Y_{T1o}, Y_{T2o}, Y_{Tmo} \right.) = \sum_{y_{11} y_{12} \cdots y_{Tm}} \frac{\prod_{i,j} p(y_{ij} \left| p_a(Y_{ij}) \right.) \prod_{i,k} p(x_{ik} \left| p_a(X_{ik}) \right.) \prod_{i,j} p(Y_{ijo} = y_{ijo})}{\sum_{x_{11}, x_{21}, ..., x_{T1} \cdots x_{Tn}} \prod_{i,j} p\left(y_{ij} \left| p_a(Y_{ij}) \right.\right) \prod_{i,k} p\left(x_{ik} \left| p_a(X_{ik}) \right.\right)}$$

$$i \in [1, T], j \in [1, m], K \in [1, n] \qquad (3)$$

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. 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 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] Dalia S. Abdelhamid, Yingyue Zhang, Daniel R. Lewis, Prabhas V. Moghe, William J. Welsh, and Kathryn E. Uhrich. Tartaric Acid-based Amphiphilic Macromolecules with Ether Linkages Exhibit Enhanced Repression of Oxidized Low Density Lipoprotein Uptake, Biomaterials, 2015.

[2] Malarkodi, M.P., Arunkumar, N., Venkataraman, V. Gabor wavelet based approach for face recognition. International Journal of Applied Engineering Research, 2013.

[3] Stephygraph, L.R., Arunkumar, N.Brain-actuated wireless mobile robot control through an adaptive human-machine interface. Advances in Intelligent Systems and Computing, 2016.

[4] Arunkumar, N., Kumar, K.R., Venkataraman, V. Automatic detection of epileptic seizures using new entropy measures. Journal of Medical Imaging and Health Informatics, 2016.

[5] Rafik Hamza, Khan Muhammad, Arunkumar N, Gustavo Ramírez González, Hash based Encryption for Keyframes of Diagnostic Hysteroscopy, IEEE Access, 2017.

[6] Dalia S. Abdelhamid, Yingyue Zhang, Daniel R. Lewis, Prabhas V. Moghe, William J. Welsh, and Kathryn E. Uhrich. Tartaric Acid-based Amphiphilic Macromolecules with Ether Linkages Exhibit Enhanced Repression of Oxidized Low Density Lipoprotein Uptake, Biomaterials, 2015.

[7] Arunkumar, N., Ramkumar, K., Hema, S., Nithya, A., Prakash, P., Kirthika, V. Fuzzy Lyapunov exponent based onset detection of the epileptic seizures. 2013 IEEE Conference on Information and Communication Technologies, ICT 2013, 2013.

[8] Jonathan J. Faig, Alysha Moretti, Laurie B. Joseph, Yingyue Zhang, Mary Joy Nova, Kervin Smith, and Kathryn E. Uhrich. Biodegradable Kojic Acid-Based Polymers: Controlled Delivery of Bioactives for Melanogenesis Inhibition, Biomacromolecules, 2017.