International Journal of Current Research and Modern Education (IJCRME)
ISSN (Online): 2455 – 5428 & Impact Factor: 3.165
Special Issue, NCFTCCPS - 2016

BAYESIAN NETWORK METHODOLOGY FOR CYBER SECURITY

P. Mohana Priya* & A. Kodieswari**
* PG Scholar, Department of Information Technology, Bannari Amman Institute of Technology, Erode, Tamilnadu
** Assistant Professor, Department of Information Technology, Bannari Amman Institute of Technology, Erode, Tamilnadu

Abstract:

Cyber security issues like cost optimization, system safety and cyber-attack are increasing nowadays due to development in technology. There is lack of sufficient information to solve these issues. The Bayesian network is one of the most popular probabilistic methodologies can be used to overcome the limitation of the issues. Two Bayesian network models have been proposed to system optimization and cyber security for specific industry control system to prepare the mobile environment. The particle swarm optimization algorithm achieves optimal mitigation measures with respect to each vulnerability in minimum search space. In these proposed models, the performance of each particle (vulnerability) is measured using a predefined fitness function, which is cost function. The experimental test conducted proves that the proposed methodology provides the better result than the existing work.

Key Words: Bayesian Network, System Optimization & Cyber Security

1. Introduction:

Industries or workers have been greatly influenced by the development of technology related to mobile systems such as personal digital assistant (PDA), mobile phone and laptop. The characteristic of mobile device provides mobility and spacious working environment to users by using it there are a few common concerns between nuclear industry and mobile device such as standardization and cost optimization with advent of new technology, safety and cyber threats. Cost optimization is important from business point of view and has equal importance in both industries. In nuclear safety, one is particularly interested in the safety of critical assets and safe operation to keep public, worker and environment safe from hazardous radiation. Using the devices based on digital technology can introduce issues such as cyber security to industrial system, especially critical infrastructure like nuclear power plant. The system optimization issue is to find out the optimal configuration of the system, caused by modernization from analog to digital system or changing the system configuration, by comparison reliability of system with cost of system. The cyber security is very important issue on industrial facilities, especially critical infrastructure control system, because it is hazardous to the public safety as well as the finance loss. We need sufficient information to solve these issues, but generally there is lack of information since it is difficult to perform the penetration test for the critical infrastructure control system.

In order to overcome these problems, we introduce the Bayesian network methodology which is one of the most popular probabilistic methodologies based on Bayesian theory The problem about lack of information can be overcome by using Bayesian network (BN). In t1, we propose two models used the BN to represent that the BN methodology can be applied to these issues. One is the optimization model by using the BN to find out the optimal point between reliability and cost of system. And other is the cyber security evaluation model to find out vulnerability and optimal mitigation measure of cyber threat.

2. Bayesian Network (BN):

Bayesian network (BN) is a directed acyclic graph (DAG) of arc to represent the dependencies between nodes, which represent the variables, using the Bayesian theory. BN is composed of node, arc and node probability table (NPT) . The node is a variable, the arc represents the cause-and-effect relationship and NPT means the probability table that summarizes the occur probability between the causal relationship nodes. BN methodology can solve problems such as lack of information, posterior inference and changing from the qualitative to quantitative problem by learning new information on the conditional probability with calculation of the relationship between the posterior and prior probability.

3. Modeling by Using BN:

To propose two represent models to find out optimal system configuration, and measure of vulnerability and optimal mitigation for cyber-attacks caused by mobile device, which applies to industrial control system (ICS) with BN for solving the lack of information issue or cyber security issue. In this paper, the subject of application is restricted to an ICS of critical infrastructure like nuclear reactor protection system (RPS). RPS in nuclear industry is important to retain the safety state when abnormal state since an accident occurs to a nuclear facility. Then, two models are developed by using BN. These models are significant with the introduction of digital, like mobile, I&C system. Bayesian network is suggested for evaluating cyber security for nuclear facilities in an integrated manner. To develop the cyber security risk model, an activity-quality analysis model was developed first to evaluate how sufficiently

A. Optimal Model for RPS Architecture:

To find out optimal configuration of system, we make several configuration of nuclear reactor protection system (RPS) as one of ICS and an optimization model to determine optimal instrumentation and control (I&C) architecture configuration in terms of availability and cost. The four cases with different architecture formation for RPS were developed with single and double redundancy of bi-stable modules, coincidence processor module, and safety or protection circuit actuation logic.

The architecture configurations are transformed to reliability block diagram based on logical operation and function of modules. The BN models for four configurations were developed to get the availability analysis by using AND gate, OR gate and N-out-of-M gate as BN functions. Cost estimation model was proposed for the architecture configurations, respectively.

BN model can be used to calculate the system reliability. For cost estimation, a numeric multiplier of X arbitrary units was assigned to each component based on experts and designers judgment and cost for each configuration was calculated.

Reliability index, which means the increase of reliability per unit of cost, is proposed by calculation of cost and availability with each configuration and a configuration of architecture that gives highest availability with maintaining low cost of manufacturing can be identified. It was found that reliability can be enhanced at the rate of 5E -05 per X unit of cost.

B. Cyber Security Risk Model for RPS Architecture:

Mobile like PDA, mobile phone and laptop technology give usability to user during maintain period of component, device and system. The cyber-attack is emphasized as new critical threat caused by applying digital device into ICS. Cyber security against cyber-attack is difficult to analysis and modeling due to lack of information like penetration test data. We suggest the cyber security risk model for RPS I&C system with the BN, it is shown in Fig. 1, to overcome these problems by calculating

of the relationship between the posterior and prior probability. The model utilizing the benefit of BN can analyze the risk that cyber-attack occurs at RPS. It can be utilized for the quantitative analysis by the proposed measure, cyber security risk as well as for various qualitative analyses.

4. Activity Quality Nodes:

Cyber security risk model is composed of the activity quality analysis model and the architecture analysis model. The activity-quality analysis model was proposed to check how people and/or organization comply with the cyber security regulatory guide. It helps to analyze the relationships of the activity-quality checklists and their influences to cyber security. The architecture analysis model was also developed for the RPS as an illustrative purpose. For the definition of the critical cyber-attack scenarios on RPS of nuclear industry, the vulnerabilities and mitigation measures were analyzed. Then, the two models, activity-quality and architecture analysis models, were integrated to cyber security risk model by using BN. Then, several analyses were performed by using the cyber security risk model for confirming the model. The analysis of the vulnerability and optimal mitigation measure against the vulnerability was performed with the assumption that a cyber-attack occurs to a maintenance and test processor in the RPS. In this analysis, prioritizing the order of vulnerabilities and reinforcing the mitigation measures were analyzed with the assumed cyber-attack to maintenance and test processor. If a cyber attack occurs at a system scale, it is important to have confidence on which component is the key element corresponding to the attack situation. This analysis proved that the developed model could provide this kind of information through the back propagation feature of the BN such as that Coincidence Processor and Intra-Channel are more risk significant than other subsystems of RPS and prioritized vulnerabilities order for RPS. Finally, the analysis of the cyber security risk and the optimal mitigation measures regarding vulnerabilities was performed on RPS. This analysis infers that the use of the cyber security risk model makes it possible to create simulated penetration test scenarios for future directions. Activity quality Node Architecture Component Node Cause Node Situation Node Accident Case Node Cyber Security Risk Mitigation Measure Vulnerability Fig. 1. The simplified cyber security risk model for RPS with Bayesian network

5. Conclusion:

For preparing the introduction of the latest devices based on digital interface like mobile on critical infrastructure facilities, we suggest the BN methodology and the two models based on the methodology to demonstrate the usefulness of the BN for specific ICSs. One is the model for the optimization of system configuration in view of reliability and cost. This model was developed for RPS and demonstrated the usefulness of the BN. Using this model, we could find out an optimal configuration by analyzing the reliability and cost of each changing configuration. The other is the cyber security evaluation model, which is also based on the BN, to analyze the vulnerabilities and the optimal mitigation measures for RPS architecture. The model found out the critical vulnerabilities and the optimal mitigation measures against the vulnerabilities for several assumed scenarios by using the BN function of back propagation calculation. The studies using these two models infer that the BN methodology can be applied to other systems like mobile systems for the same purposes.

6. References:

1. Lee, H.C., Lee G.B.: Prototype of Operator Interface for Monitoring and Controlling in the Mobile Control Room. Proceedings of the 2013 ACM international conference on interactive tabletops and surfaces, pp 305-308

(2013)
2. Kai Ji, Tian-Jian Li: Detection and Analysis of Unidirectional Licks in Mobile Ad Hoc Network under Nuclear Power Plants Environment. Emerging Technologies for Information Systems, Computing, and Management Lecture Notes in Electrical Engineering Volume 236, pp 871-878 (2013)
3. Heckerman D.: A tutorial on learning with Bayesian networks (1996)
4. Rahman K., Shin J.S., Heo G.Y., Son H.S.: Reliability Analysis of I&C Architecture of Research Reactors Using Bayesian Networks, Korean Nuclear Society Autumn Meeting (2013)
5. Shin, J.S., Son H.S., Rahman K., Heo G.Y.: Development of Cyber Security Evaluation Model Using Bayesian Networks, Reliability Engineering and System Safety (submission, 2013)
6. Shin J.S., Son H.S., and Heo G.Y.: Cyber Security Risk Analysis Model Composed with Activity quality and Architecture Model. International Conference on Computer, Networks and Communication Engineering, p. 609-612 (2013)