Proceedings of the 3rd International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/6/20230931

Intelligent network management model based on Bayesian network

Haoqiang Shi

University of California, Santa Barbara, Santa Barbara, CA 93116

haoqiangshi@ucsb.edu

Abstract. Nowadays, with the vigorous promotion of digital applications, major enterprises have established their own enterprise networks, in which there are many network equipment, communication lines, servers and various applications. To ensure the stable running of the network system, the enterprise establishes a special network management system to monitor the network running status. The network management system can detect all kinds of network faults, such as line interruption, port down, and service application exception alarms. However, the usual network management system can only discover and deal with the faults that have occurred, and lack to predict and judge the equipment or application system that may have problems. This paper discusses the establishment of an intelligent network management model that links the log system and the alarm monitoring system based on the Bayesian network. By collecting and processing the logs of all devices and applications in the network, based on the alarm information, people can calculate the probability of network devices, communication lines, and service applications that may be faulty to predict network faults in advance and improve the security performance of the network system.

Keywords: network management, log system, alarm information, Bayesian network, fault prediction.

1. Introduction

The security and dependability of the communication network are becoming more and more crucial as a result of the Internet's quick expansion. How to effectively manage the network is a hot issue. Numerous devices and systems in the network will produce a large amount of log information, which is of great value for understanding the status and performance of the network. At the same time, due to the high connectivity of the modern network structure, when there is a failure somewhere in the network, the equipment associated with it will also cause the corresponding failure, and generate a large number of alarm information in a short time. The ability to quickly analyze log and alarm data, accurately locate faults, and troubleshoot them is essential for network management. At present, most network management systems have low correlation between the log system and the monitoring alarm system, the monitoring threshold is set by manual, the accuracy and sensitivity are insufficient, and they can only deal with the faults that have occurred, and the hidden dangers of faults cannot be effectively predicted. In order to evaluate network log data, Min Du et al. offer DeepLog, a deep neural network model using Long Short-Term Memory (LSTM).[1] [2]. To realize the anomaly detection of network system, Cheng Hong proposed a method of network fault detection and

DOI: 10.54254/2755-2721/6/20230931

maintenance by building a computer network fault detection model based on BP neural network and relying on fault detection algorithm [3]. However, the fault prediction method based on neural network has some problems, such as large amount of calculation, long learning time, and difficult to interpret the output results [4]. Therefore, this paper proposes an intelligent network management model based on Bayesian network to optimize the solution of the above problems. By analyzing and filtering the association rules of alarm information and log data, the processed data is sent to Bayesian network learning as input to calculate the probability of failure of network equipment, communication lines and service applications at a certain time, so as to realize the prediction of network failure, solve the problem of low accuracy of network equipment failure prediction, and improve the security performance of network system. Bayesian network is a kind of probabilistic network. Bayesian network based on probabilistic inference has great advantages in solving faults caused by uncertainty and correlation of complex equipment [5].

2. Basic concept of Bayesian

The formula for estimating conditional probability was first proposed by British scholar Bayesian (1702–1761) in the early 18th century to address the following types of problems: assuming H[1], H[2]... An event A and H[1], H[2], and H[n] are mutually exclusive and make up a full event, and their probabilities P(H[i]) (i=1, 2... With known conditional probabilities P (A | H [i] and P (H [i] | A), H[n] is generated at random.

Expression of the Bayes formula:$P(A|B)=\frac{P(B|A)P(A)}{P(B)}$

P (A | B) is in B under the condition of the possibility of A. Before the occurrence of event B, we have The prior probability of A, denoted by P(A), is a fundamental probability estimate for the occurrence of event A. When event B occurs, we perform a new assessment of the probability of event A, denoted by the posterior probability, expressed in P(A | B). Prior to the occurrence of event A, we have a fundamental probability judgment for the occurrence of event B, known as the prior probability of B, denoted by P(B).

Judea Pearl first proposed the Bayesian network, a probabilistic graph model, in 1985[4]. It is a type of uncertainty processing model that mimics causality in human thought processes. Its network topology is a directed acyclic graph (DAG). The nodes in the directed acyclic graph of the Bayesian network represent random variables, or X1, X2,..., Xn, which can be variables that are visible to the eye, variables that are hidden from view, parameters that are unknown, etc. When connecting variables and claims that are thought to be causal or not conditionally independent, arrows are used. A conditional probability value is generated when two nodes that represent the "Cause (Parents)" and the "Result (Children)" are connected by a single arrow. For instance, if node E directly influences node H, as shown in the figure below, then using the arrow from E to H the nodes E to build H directed arc (E, H), weights (i.e., the strength of the connection) with the conditional probability P (H | E) would be appropriate.

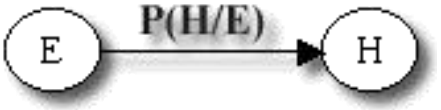

Figure 1. A directed acyclic graph with two nodes.

In essence, a Bayesian network is created when random variables used in a particular research system are independently constructed in a directed graph based on the presence or absence of conditions. Mostly, conditional dependencies between random variables are described by this term. Circles stand in for random variables, while arrows represent conditional relationships.

A directed acyclic graph (DAG) is the definition of a Bayesian network. Now consider the definition of X as a Bayesian network. In this case, "I" stands for the collection of all nodes in the graph, "E" for the collection of directed linked segments, and "X" for the random variable signified by node I in the DAG. If the joint probability of node X can be expressed as:

DOI: 10.54254/2755-2721/6/20230931

When X is compared to a directed acyclic graph G, it is referred to as the Bayesian network, with pa standing for the "cause" of node i. Or, pa (i) is "i's" parent. In addition, the joint probability of any random variable can be obtained by multiplying the respective local conditional probability distributions.

$p(x_1,\ldots,.x_k) = p(x_k|x_1,\ldots,.x_{k-1})\ldots p(x_2|x_1)p(x_1)$

As shown in the figure below,

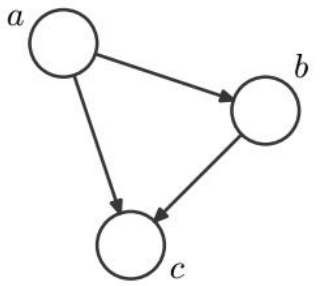

Figure 2. simple Bayesian network.

Because a leads to b, and a and b lead to c, so there are;

$p(a,b,c) = p(c|a,b)p(b|a)p(a)$

3. Application of Bayesian network in network management

The three steps involved in creating a Bayesian network are: defining the variables; learning the structure; and learning the parameters. Although these three jobs are often carried out in order, it is frequently required to compromise between the following two factors during the construction process. One the one hand, a sufficiently large and rich network model must be constructed in order to achieve sufficient accuracy. On the other hand, taking into account the expense of developing and maintaining the model as well as the complexity of probabilistic inference, it is actually common for the aforementioned three processes to interact iteratively and repeatedly when creating a Bayesian network.The second three tasks, which include creating a directed acyclic graph and specifying the distribution parameters for each node in the graph (each node corresponding to a conditional probability distribution table), are the important components and challenges of building a Bayesian network.To characterize the causal connection between many events, the Bayesian network (Bayesian network) can create statistics based on expert expertise to create conditional probability (A=i B=i). According to the Bayesian theorem, P (AB) = P (B | A) P (A)/P (B), the construction of Bayesian networks is based on the graph model, with the entire complex system being constructed to express it in every conceivable circumstance. Nodes represent random variables in the directed acyclic graph, arrows conditional dependencies, and directed edges indicate causal links. By adding all all dependencies, the conditional probability distribution graph is created.In theory, given the conditional probability table and the network architecture, any query can be obtained by repeatedly applying the Bayesian formula and the product and sum formula.

DOI: 10.54254/2755-2721/6/20230931

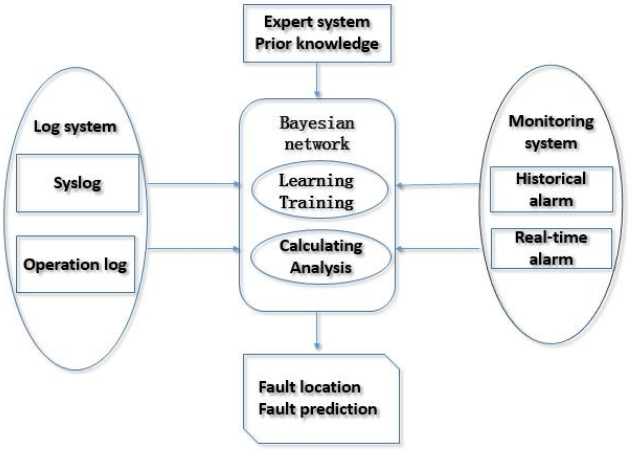

Figure 3. Network Management Model Based On Bayesian network.

3.1. Attribute variables of network management system in Bayesian model

Table 1. System logs are classified according to network attributes, horizontal partitioning and vertical layering.

Variable	Area		Variable	Class		Variable	Class
X1	Core area		Y1	Network equipment		Z1	Operating system
X2	Access area		Y2	Network line		Z2	Database
X3	Swap area		Y3	Network port		Z3	Middleware
X4	DMZ		Y4	Network protocol		Z4	Application system

Table 2. Operation logs are classified into read operation logs, write operation logs, and resource operation logs.

Variable	Operation type	Description
R	Read operation	Such as login, logout, view...
W	Write operation	Changes, upgrades, resets...
Re	Resource manipulation	Create or delete a resource

DOI: 10.54254/2755-2721/6/20230931

Table 3. According to the severity of the fault, the alarm information is classified.

Alarm level	Definition	Description
1	Critical	This level of failure affects the services provided by the system and requires immediate action. If a device or resource is completely unavailable, recovery is required, even if the failure occurs during non-working hours, immediate action is required.
2	Major	Failures of this level affect the quality of service and require urgent action. If the service quality of a certain equipment or resource is degraded, it needs to be restored and restored to full capacity, and measures need to be taken immediately within working hours.
3	Minor	Failures of this magnitude have not yet affected quality of service, but they need to be addressed or further observed when appropriate to avoid more serious failures。
4	Warning	Such level of fault indication may have potential errors affecting the provided service and the corresponding measures are handled according to different errors.
5	Indeterminate	The level of the alarm cannot be determined, that is, the impact caused by the alarm depends on the actual environment.
6	Cleared	Indicates the removal of one or more previously reported alarms. This level of alarm clears all alarms with the same alarm type, probable cause, and specific problem for the managed object. Multiple associated advertisements can be deleted by configuring the advertisement parameters associated with each other

3.2. Bayesian network learning

The Bayesian learning theory is a perfect model for data mining and the representation of uncertain knowledge since it integrates previous knowledge with sample information, dependency with probability representation, and so on. Directed acyclic graphs and conditional probability sets are the two fundamental ideas that Bayesian networks primarily introduce. A directed acyclic graph's nodes are features and categories, and its edges are the connections between those two types of entities that are not independent of one another. Conditional independence, or the idea that a node is independent from other nodes given the condition of its parent node, is the key idea behind a conditional probability set. Three techniques exist for Bayesian networks to learn.

Complete learning. In this way, human subjective factors totally define the Bayesian network's parameters and structure.

(2) Partial learning. In this manner, human subjectivity is used to define the node a Bayesian network's variables, and a vast amount of training data is then used to learn the structure and parameters of the network. This strategy is entirely data-driven and very flexible;

(3) Combining the above two methods, The domain experts define the node variables in the Bayesian network, and their expertise also specifies the network's structure. The network's parameters are then trained from the data using a machine learning technique. The conditional probability distribution of each node is calculated using a Bayesian framework as part of the parametric learning process. When a Bayesian network is subjected to probabilistic inference, it is assumed that values A,

DOI: 10.54254/2755-2721/6/20230931

B, and F are seen but G is unknown. The value G is derived using a Bayesian network using the values A, B, and F.

3.3. Algorithm

(1) Choose every variable. Create a group of variables called Vi in a Bayesian network that corresponds to each node in the fault propagation model and whose value domain is {abnormal, normal}.

(2)Create the topology for the Bayesian network. A directed edge Y → X of the Bayesian network is specified for each directed edge Y → X in the fault propagation model, indicating that node Y is the parent node of node X and that X and Y are somewhat dependent on one another. A Bayesian network model must be created for each defect category in order to perform fault diagnosis. The conditional probability of the node where the fault occurs is assessed in order to realize the fault category diagnosis because there are numerous causes of the problem.

The Bayesian network has excellent learning capabilities. Bayesian network learning is the process of identifying the network that can most closely match a given training sample set. The network log data is constantly expanding in real-world applications, and the Bayesian network can retrain using new samples, improve the network's structure, and adjust its parameters as needed to more effectively mine the network log. [6].

4. Conclusion

With a focus on the problem of how to effectively predict computer network failure, this paper proposes an intelligent network management model based on a Bayesian network. Firstly, the alarm information and log data are analyzed and filtered by association rules, in which the system log is classified according to the horizontal and vertical layers of network attributes, and the alarm information is classified according to the severity of fault. Second, the cleaned data are fed into the Bayesian network for learning, and on the basis of the network's analysis, various attribute values are added to increase the accuracy of the Bayesian network's probability prediction. Using the fault prediction model of the Bayesian network, the network can be continuously updated to complete the accumulation of knowledge, so as to improve the prediction results and improve the security and reliability of computer networks. This is done by studying the existing log information and alarm information. The Bayesian network is the perfect model for data mining and the representation of uncertain knowledge because it combines prior knowledge with sample data, a dependence connection with probability representation, and a dependence relationship.The Bayesian network offers numerous advantages over other data mining techniques like rule representation, decision trees, and artificial neural networks. For example, combining a Bayesian network and Bayesian statistics can make the most of domain knowledge and information from sample data. When a variable has a missing value, for example, other methods' predictions will deviate greatly, but Bayesian networks, which offer a more logical probability association model, can produce accurate predictions. As a result, Bayesian networks have a significant role and potential in real-world applications.

References

[1] F. V. Jensen. An introduction to bayesian networks and decision graphs. Technical report, Springer, New York, 2001.

[2] Min Du, Feifei Li, Guineng Zheng,Vivek Srikumar. DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning.CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications SecurityOctober 2017 Pages 1285–1298)

[3] Cheng Hong Computer network fault detection method and maintenance strategy based on BP neural network. ISSN 1009-3044 Computer Knowledge and Technology Computer Knowledge and Technology Vol.15, No.7, March. 2019

[4] JAUDET M, IQBAL N, HUSSAIN A. Neural networks for fault-prediction in a

DOI: 10.54254/2755-2721/6/20230931

telecommunications network INMIC, 2004: Proceedings of the 2004 8th International Multitopic Conference

[5] Wichlund K Y,Sordalen O J, O.Egeland.Control properties of underactuated Vehicles[C] Proc IEEE Int Conf on Robotics and Automation，1995：2009-2014.

[6] Chen Jiamin. Research and Implementation of Network log mining using Bayesian Network [D]. Soochow University,2008.