Priority-based hierarchical inference rules algorithm for alarm correlation

Guannan Si[1], Guang Yang[2], Hairong Xiao[3]
Shandong JiaoTong University
Jinan, China
siguannan@163.com

ABSTRACT: An abstract model of the logical relationship among the alarm and algorithm based on hierarchical priority alarm correlation inference rules are proposed by analysis of existing alarm correlation needs. The algorithm clearly describes the relationship and alarm, and can be flexibly combined multi-part configured to expand coverage area of the algorithm rules. It is in favor of knowledge update in change process of the network structure.

Key words: Alarm correlation, Inference Rules, Network Structure

Received: 3 September 2016, Revised 1 October 2016, Accepted 15 October 2016

1. Introduction

With rapid development of mobile communication industry, communication network scale unceasingly expands, complexity of network is more and more high. In order to ensure safety of telecommunications networks, stable and reliable operation, fault management function in network management attracts more and more attention of the network operation Department. When a fault occurs in the network, to judge fault reason, nature and location as soon as possible is a key prerequisite for troubleshooting. However, the communication line among devices are interrelated in a complex telecommunications network, faults of a device or a line often cause related multiple devices or multiple lines generating a large number of alarm information at the same time, which makes network fault diagnosis becomes very complicated.

The best way to solve the problem above is to adopt analysis method of alarm correlation. Alarm correlation analysis is to combine multiple related alarm through mergers and transformation, in order to make it become a few alarms containing more fault related information. So that the number of reporting alarm is declined, and network operation and maintenance personnel's

work burden is also reduced. It also helps to identify the fault position and reason in the shortest time and eliminate the fault in time in order to restore normal business transmission. So alarm correlation analysis has attracted more and more researchers to explore in the technology and theory. It mainly includes following methods:

(1) Alarm correlation based on case reasoning [1-3]. Experience problem solutions are stored in case base. When meeting the question, people can search the case base for similar solution case at any time, in order to obtain current problem solving method. The advantage of this method is relatively easy to build the case base, simple and fast in solving problems and high efficiency, with the ability to self-learning and self-organization. However, this method does not have the versatility to be tailored for each application areas, on the other hand associated with processing capabilities for real-time alarm insufficient, and there is no theoretical basis for the strict sense.

(2) Alarm correlation based on artificial neural network [4, 5]. Its neural network is trained by using the network device alarm information and the actual network fault conditions to enable them to identify the specific fault. Its characteristics are fault tolerant, capable of self-learning, self-organization and adaptive. But it takes a long time training, after training artificial neural networks are often difficult to interpret their results.

(3) Alarm correlation method based on code [6]. It is performed through the establishment of potential problems (failure) and the characterization of these issues symptoms (warning) of incidence matrix and use it to locate the problem. Code based alarm correlation method is simple, wide application range, speed, but the method is not good enough adaptability, code design and modification requires human involvement, intelligence is not high.

(4) Alarm correlation based on data mining method [7-10]. It introduces data mining technology into alarm correlation, and reveals the hidden rules of meaningful knowledge and information in the sign behind the massive failure of the original low-level, so that network managers can quickly locate faults and make further decisions and failures forecast. Using data mining methods better able to adapt to alarm correlation dynamic changes of the network, and can use a large number of outstanding mining field method to identify hidden rules in the event log. However, this rule is too trivial, but the law can only reflect the local area, it needs to be combined with other methods for processing in order to achieve better results.

(5) Alarm correlation based on inference rules [11, 12]. The alarms correlation knowledge is organized into a set of rules, which rules the current state of the system using a rule-based inference mechanism to determine the system should be implemented. “Identification - movement” cycle is repeated to satisfy all of the rules match the current state until no matching rule. Inference rules based alarm correlation method is intuitive, flexible and easily to be handled in reasoning modular. This method is particularly suited to address those covering an area of small, relatively stable and unchanging, has been well understood in the field.

This paper analyses of existing alarm correlation demand, the model of abstract logical relationship between the alarm and proposed algorithm based on hierarchical priority alarms associated inference rules. The algorithm clearly describes the relationship between alarms, and can be flexibly combined multi-part configured to expand the coverage area of the rules of the algorithm, the process in favor of the change in the structure of the network to update their knowledge.

2. Requirements of alarm correlation analysis

Alarm correlation analysis is association and association rules alarm communication between network resources, information related to the processing of alarm in time and space, in order to reduce the number of alert messages. To help maintenance personnel faster and more effectively deal with important alerts and alarms originating accurately locate the alarm occurs, the alarm grasp the impact on the network, accelerate the processing speed alarms and faults, improve maintenance efficiency. According to the maintenance staff to summarize the experience and actual operation and maintenance needs, there are currently eight alarm correlation analysis needed. They are listed as follows:

(1) Correlation between relay alarm and trunk group alarm. A trunk group alarm relay alarms within all depend on this trunk group, from another perspective, the relay alarms can be derived from the trunk group alarms.

(2) Correlation between Signaling link alarm and signaling link set. A signaling link set alarm rely on all the signaling links alarm with in this signaling link set. It can also believe that signaling links alarm can derive signaling link set alarm.

(3) Correlation between signaling link set alarm and destination signaling point cannot reach alarm. Unreachable destination signaling point alarm rely on this signaling route carries all the signaling link set an alarm, it can be said, to the same destination signaling point of all alarm signaling link group can derive out of service destination signaling point unreachable alarm.

(4) Correlation between trunk group alarm and traffic routing alarm. Routing traffic alarm rely on this traffic routing trunk group carrying all alarms.

(5) Correlation between relay alarm and signaling link alarm. Relay alarms can derive signaling links alarm running on this relay.

(6) Correlation between relay, relay group local end alarm and away end alarm. If the relay, relay group local end alarm is generated, and the relay, relay group away end also produces an alarm, we define them homologous relationships.

(7) Correlation between signaling link, signaling link set local end alarm and signaling link, signaling link set away end alarm. At the same signaling links, signaling link group of local produce alarm, this signaling link, the peer group is also bound signaling link generates an alarm, alerting us to define these two homologous relationships.

(8) Correlation between destination signaling points cannot reach alarm. When different switches issued to the same destination signaling point cannot reach alarm, the alarm will be defined as homologous relationships.

3. Design of priority-based hierarchical inference rules algorithm for alarm correlation

Previous analysis of the need for alarm correlation analysis of alarm types can be summed up alarm correlation characteristics as follows:

• **Priority:** Each alarm may vary depending on a variety of association rules associated with other alarms, rule execution order is determined by priority.

• **Exclusion:** the existence of mutually exclusive characteristics between certain rules. For the same after the alarm has been performed a rule no longer perform other rules of exclusion rule.

• **Sequential:** applied with a warning of more than one rule is always executed in a certain order.

Based on the above characteristics for alarm correlation analysis is designed based on hierarchical priority alarm association rules of inference algorithms, both to adapt to these characteristics, but also for flexible configuration, but they can adapt to changes in network structure. As Figure 1 shows:

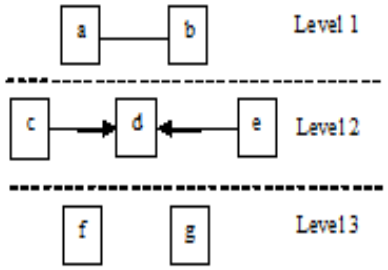

Figure 1. Priority-based hierarchical inference rules algorithm

Rules can be divided into two parts, rule body and rule item, which are stored in rule body table and rule item table. A rule body corresponds to one or more rule items. Rule body is used to define alarms that rules can be applied. Rule item is used to determine if the selected rule can perform in current system state. Rule description is shown in Figure 2:

Inference rules algorithm for alarm correlation are as follows:

All rules are divided into a number of priority, high priority rules exclude low priority rules, that is, an alarm has been used for high-priority rule is no longer a low-priority rules for its application.

Rule 1:
Rule body: Alarm correlation of signaling link and relay circuit
Rule item:
1. Local end network element names are the same
2. Away end network element names are the same

Figure 2. Rule description

No priority rules between the same connections showed mutually exclusive, that is, for an alarm applications in which a rule is a rule cannot be applied another.

Represents a linear coupling between the two rules are not mutually exclusive same priority rules, that is, for applications in which an alarm rule can also be applied another rule.

A linear coupling with an arrow between the same priority rule, the exclusion rule along the direction of the arrow pointing in the direction, that is, the rule in arrow tail excludes the rule in Arrow head.

Alarm correlation is divided into “search” and “execute” two-step operation. When there is a need for alarm alarm correlation analysis, the first from the rule base can be used to retrieve the alarm association rules, assumed to be a, d, f, g. Then determine the rules need to be performed in accordance with the rules of the current term. It is described by following three cases:

The current rules a, d, f need to be performed. First priority order execution rules a, due to a highest priority, so if they meet the conditions associated with low-priority alarms application in accordance with the rules (eg: c, d, e, f, g), these rules continue. If the rule d has been used, due to the rules of a, b are not mutually exclusive, a rule can continue execution. Exclusion of low-level rules under the rules of the high-level features, when executed after a rule is no longer enforce the rules d and f.

The current rules d, f, g need to be performed. Performed first in order of priority rule d, if they meet the conditions associated with low-priority alarms application rules (such as: f, g), this rule continue. If they meet the conditions of alarms associated with the application through the same priority rules (eg: c, e), in accordance with the rules of exclusion direction, these alarms are no longer apply this rule. If you comply with the conditions associated with the high-priority alarm application rules (eg: a, b), these alarms are no longer apply this rule. Exclusion of low-level rules under the rules of high-level features, when executed after d f no longer enforce the rules and the rules of g.

The current rule f need to be performed. If they meet the conditions associated with the alarm application had priority rules (eg: g), due to the rules of f, g mutually exclusive, these alarms are no longer apply to this rule. If they meet the criteria associated with the high priority alarm application rules (such as: a, b, c, d, e), these alarms are no longer applied to this rule.

4. Experiment and verification

4.1 Alarm Correlation Process Flow Design

Alarm information processing is divided into clearing and activities, but after the alarm information is collected, the need to determine whether the alarm status flag is cleared or activity, and then enter the appropriate processes.

The process is described as follows:

(1) Active alarm process

According to the alarm status flag judgment for activities alarm when enters the active alarm process. Firstly, the alarm text is analyzed, positioning information can be got from alarm text, such as network element alarm signaling point codes and so on. Basic information obtained after the network element alarm, you can query this information from a network resource database to richer information, such as peer network element name, relay port number, circuit code, in order to pinpoint the fault location.

After detailed location information, according to the alarm association rules in line with the title of the query, save relationship cycle applications association rules corresponding alarm, and the alarm between. Show alarm information and relationship to the user upon completion.

(2) Cleaning alarm process

It will enter judgment cleaning alarm process according to the alarm status symbol for cleaning alarm. Serial determined according to the alarm system alarms need to be cleared, the corresponding alarm will be removed from the active alarms table and inserted into the alarm history to the table, and delete alarms associated with that relationship. Alarm information and the relationship of the user interface will be cleaned when it is completed.

4.2 Architecture of Alarm Correlation Subsystem

As a subsystem of communication line management system, alarm correlation analysis subsystem using C/S architecture, the background using C++ language development, foreground using C#.Net development, between the front and back using Tuxedo middleware for communication, as Figure 3 shows:

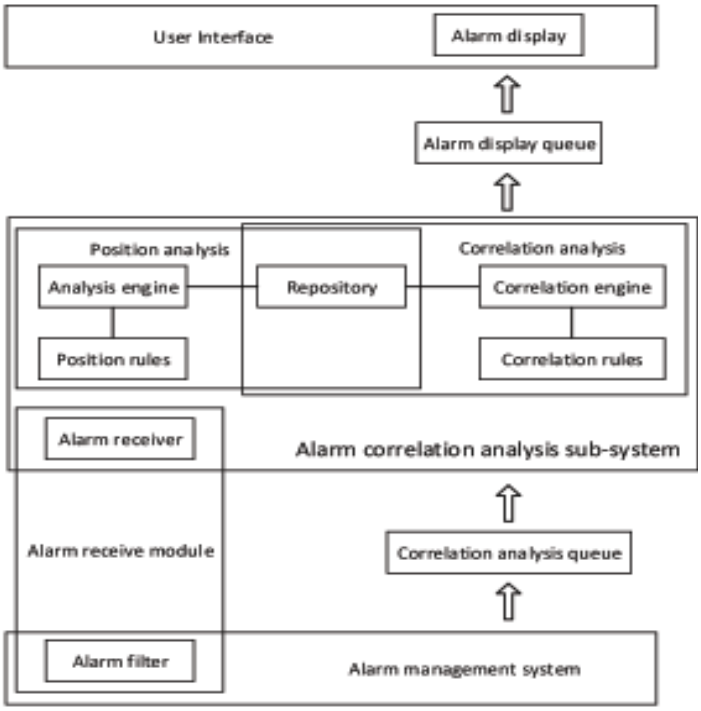

Figure 3. Architecture of alarm correlation subsystem

Alarm receiving module normalization alarm information processed, remove the alarm's title, manufacturer, grade, network element name and all alarms have general information to a unified treatment of all alarms. Positioning analysis module based on certain rules to obtain the original text from the alarm information they need to determine the location of network elements through the repository network element information, analyze the relationship between network elements for analysis and check the alarm association preparation. After the association analysis module to get location information, search in the rule base the qualifying rules, the search is successful execution of operations in accordance with predefined rules, alarm correlation analysis. After the analysis is complete pushed the alarm display queue, send forward units for display.

4.3 Module Design of Alarm Correlation Subsystem

(1) Alarm receive module

Alarm correlation analysis receiver module is the interface between the subsystem and the communication line management system background, is divided into two parts, filter alarms, alarm receiver. Alarm filters embedded in the communication line management background, the need for correlation analysis for alarm filtering. Since not all need to be alert correlation analysis, thus alerting the filter configuration file selected in accordance with the need for alarm correlation analysis, correlation analysis and pressed into the queue. Alarm receiver removed from the queue to analyze alarms, key segments of the necessary processing to conform to the rules need to locate analysis.

(2) Position analysis module

Because only a few simple relationship between alarm events, for more complex analysis of the association must be by means of the relationship between resources, positioning analysis became the basis for alarm correlation analysis. First, location analysis to determine the local network element alarm, peer network element, signaling link number, trunk port number and other information in order to pinpoint the alarm to the resource. Then, based on the location information by association rules and correlation analysis between resources, to achieve the associated alarm handling.

Location information is obtained by analyzing the original alarm because the alarm original is the most original, the most basic information alarm equipment generates, so use to obtain location information is the safest, most reliable. In positioning the rule base for each alarm define each device manufacturers to obtain location information of the rules, since the original manufacturers of different types of warning alarms are unified, so for each alarm requires only one rule to obtain location information. Each rule corresponds to certain rules, of which defines the values need to get the original from the alarm (eg: the name of the local NE, NE peer name, etc.) and value (such as: the first few lines taken from the first few byte, take the corresponding value of a field, etc.), conducted in accordance with specific rules. Location analysis engine queries to the qualifying rules, to obtain entry accordance with the rules according to the alarm from the alarm key information specified in the original, and then get richer location information by querying the repository, which completed the implementation of a positioning analysis.

(3) Alarm correlation analysis module

It mainly includes correlation analysis engine and the associated rule base in two parts. Obtained from the correlation analysis engine positioning analysis module analyzes a good location information, and in contrast with the association rules library association rules, in accordance with the aforementioned association alarm processing algorithm to select the association rules in line with the conditions of its implementation, and finally get the associated post alarm information.

(4) Alarm display module

This module is used to display the associated alarm information embedded in the foreground as a sub-module communication line interface management system. Display the alarm message displayed by way of the tree level and represents the association between alarms. In front of the parent alarm has a "+" identifier, when clicked can expand the following sub-alarm can be folded up and then clicked in order to provide a clear alarm correlation for monitoring personnel rendering interface.

5. Conclusion and future work

Based on the analysis of existing alarm correlation demand, based on the proposed priority-based hierarchical alarm correlation rules of inference algorithms, combined with specific application to establish a platform for alarm correlation analysis and put into practical operation. The results show that the algorithm can effectively analyze the relationship between alarms and provide clear presentation of alarms association for monitoring personnel. The downside is that, association rules provided mainly by professional administrators, systems lack the self-learning ability. System lacks rule memory, unable to take advantage of previous experience and knowledge. Future research directions are added to the alarm data of data mining, by analyzing the historical communication network alarm data, found that the alarm information between potential association rules, and in accordance with these rules to analyze and predict network equipment failure may occur.

Acknowledgments

The paper is supported by Natural Science Foundation of Shandong Province under the Grant (ZR2013EEM006) and Foundation of Shandong Jiaotong University under the Grant (Z201304)

References

[1] Lewis, L. (1993). A Case-Based Reasoning Approach to the Management of Faults in Communication Networks. *Proceeding IEEE Infocom'93,* 3. San Francisco. p.114-120.

[2] Lewis, L. (1996). Implementing Policy in Enterprise Networks. *IEEE Communications Magazine*.

[3] Burns, L, Hellerstein, J.L, Ma, S et al. (2001). Towards Discovery of Event Correlation Rules. *In:* IFIP/IEEE International Symposium on Integrated Network Management, Seattle, WA, USA. p.345-359.

[4] Su, L. M., Hou, C.Z., Dai, Z.J., et al. (2002). A Neural Network Apporach to Alarm Correlation. *Journal of Beijing Institute of Technology*. 22 (3) 297-299.

[5] Zhang, X.F., Hou S.Z. (2009). Alarm correlation analysis for monitoring system in power communication network. *Telecommunications for Electric Power System*. 30 (1) 47-50.

[6] Kliger, S. ,Yemini, S.,Yemini ,Y. (1995). A coding approach to event correlation, *In:* IEEEÿIFIP International Symposium on Integrated Network Management, IV(ISINM'95) p. 266-277.

[7] Li, Y.Z., Sun Y., Luo J.S., (2006). Application of WINEPI Mining Algorithm in IDS. *Computer Engineering*. 32 (23) 159-161.

[8] Liu, K.P., Li Z.Z., 2003. Frequent Episode Rule Discovery in Network Alarm Sequence. *Mini-Micro Systems*. 24 (5) 891-894.

[9] Marilly, E. Aghasaryan. (2002). Alarm correlation for complex telecommunication networks using neural networks and signal processing. p. 3-7.

[10] Cronk, R.N., Callahan, P.H., Bernstein, L. (1988). Rule Based Expert Systems for Network Management and Operations: An Introduction. *IEEE Network,* 2 (5) 7-21.

[11] Li, Z.Z., Zhu H.P., et al. (2001). Design and Implementation of a Network Fault Diagnose Expert System for Network Management. *Computer Engineering and Applications*. 37(17) 24-26.

[12] Liu, K.P., Zhu, H.P., et al. (2002). Study and Implementation of Alarm Correlation and Fault Diagnosis Expert System. Computer Engineering. 28 (6) 11-12, 68.