IOP Conf. Series: Materials Science and Engineering **719** (2020) 012018 doi:10.1088/1757-899X/719/1/012018

Alarm Filtering Method of Power Communication Network Based on Correlation Set

Shengchao Yan[1] and Lei Li[2]

[1] Nari Group Corporation/State Grid Electric Power Research Institute, PRC.
[2] State Grid Hubei Electric Power Co., Ltd. Information Communication Branch, PRC.

Abstract. In order to find out the root from a large number of alarms of alarm events, we did a good study on the alarm's characters of power communication network equipments, through which we found the alarm relevance sets. On this basis, we present a relevance-set based alarm filtering approach, which make the unnecessary and none-root alarms filtered much more quickly.

1. Introduction

System structure design Alarm correlation analysis is an effective method for root alarm analysis. At present, there are some breakthroughs in the research of alarm correlation analysis technology at home and abroad, such as data mining [1], association rules [2], pattern matching [3], signal flow [4], event tree [5] and other cutting-edge technologies, and some useful results have been achieved. In the literature [6-8], the layered filtering mechanism [7], search tree [8] and other technologies are used to filter a large number of alarms, and some practical results have been achieved in the application.

Through the in-depth study of power communication network equipment alarm, combined with its characteristics, find and sort out the alarm correlation set rules, and realize the alarm filtering technology based on the combination of alarm correlation. So as to realize the alarm filtering of alarm tide events in power communication network, eliminate the secondary and non-fundamental alarms in a large number of alarms, and provide the basis for fault location and processing of power communication network.

2. System Structure Design

The system consists of two parts. The first part: the collection of alarm filtering rules, which can realize the sorting of alarm rules commonly used in communication network, and the application of rules in the specific correlation analysis.

Fig.1 System Architecture

The second part: correlation analysis engine. Call correlation set rules to analyze the correlation of a large number of alarms, and filter the secondary and non-root alarms under the control of time folding window. The structure diagram is shown in Figure 1.

If a large number of alarm information is collected in a certain period of time, it needs to be filtered first and then submitted to the correlation analysis engine for analysis; if a simple and small amount of alarm information is collected, it will be directly sent to the correlation analysis engine for analysis and processing.

3. Rule Set of Alarm Filtering

3.1. Set Model of Alarm Filter

Alarm filter is realized by alarm filter, which is built on a mathematical model. The description of the mathematical model is shown in Formula (1) as follows.

$$[A,B,C,D]\rightarrow A \quad \text{or} \quad [A,p(A)\notin H]\rightarrow \phi \tag{1}$$

Where: a represents the alarm information of a certain group or a certain group that is monitored, P (a) refers to all parameter sets involving alarm a that may be determined as fault event, and H is the set of legal parameters and conditions that constitute the event.

It can be seen from the above formula that if the P (a) value of alarm a does not belong to the legal parameter and condition value set h, but belongs to the empty set, these alarms will be filtered out by the filter, so as to delete the alarms that do not meet the requirements of alarm correlation. The filter function block diagram is shown in Figure 2.

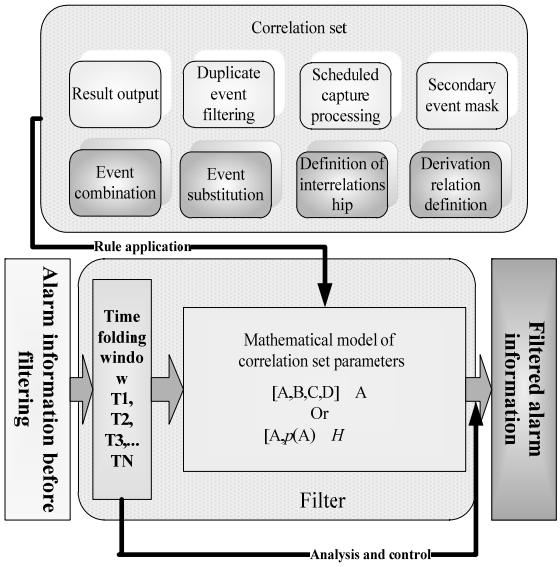

Figure 1. System Architecture

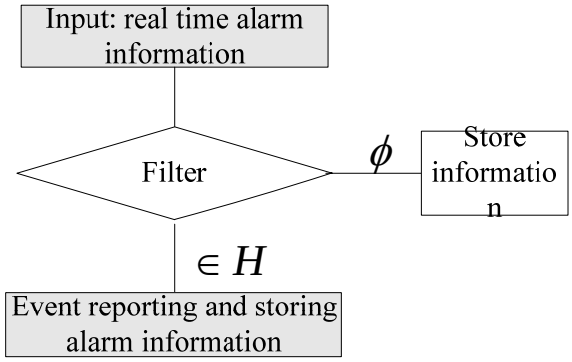

Figure 2. Alarm filtering Diagram

3.2. Alarm Filter Rule Category

The P(a) function is a set of conditions for alarm notification and event reporting. It is constructed by system settings according to various correlations, and it is used to determine which events can be reported or which events can not be reported. The system supports the setting of one or more combined alarm filter conditions. The main filter conditions set in this article are:

(1) low level alarms in pairable alarms (events): events with different alarm levels but the same other parts are called pairing alarms (events). Pairing events can be treated as a combination to clear and filter out the low-level alarms in pairing. For example, there are three alarms in an SDH device, and the alarm levels are: general alarm, main alarm and serious alarm. In this case, general alarms can be filtered, leaving major and serious alarms.

(2) false event filtering: filter mutually exclusive events and ultra short recovery events.

(3) repeat event filtering. Filter recurring events over a period of time.

(4) scheduled event capture: filter alarm events that do not meet user-defined conditions. For example, if the analog threshold of communication DC power supply voltage is set to 54 V, all alarms below 54 V will be filtered.

(5) secondary event shielding: filter the secondary alarm events that do not affect the normal operation of the equipment.

(6) event derivation filter: filter the accompanying alarm. Using the inferential relationship between events, we can filter the accompanying alarms.

The priority of these filters is defined as: false event filtering > repeated event filtering > scheduled capture processing > secondary event screening > Event derivation. Although the filtered alarm information will not be subject to subsequent intelligent analysis, its data still exists in the system database and can be queried and counted when necessary.

After the alarm filter, a large number of low-level, false, repeated, below threshold, secondary and accompanying alarms are filtered. From the actual operation, the filtration ratio can reach 50%. The remaining high-level, true, out of limit and main alarms are sent to the second part of this article: correlation analysis engine to analyze the correlation of alarms.

4. Correlation Analysis Engine

In practical application, if we directly deal with a large number of filtered alarms, then: first, the workload is large and the analysis time is long; second, there is no correlation between some alarm groups and other alarm groups at all, and the combination analysis of them has no effect and affects the analysis accuracy. Finally, the relationship between the source and the cause of the alarm can not be determined in a short time, the analysis is of low intelligence, and the work efficiency is difficult to meet the requirements.

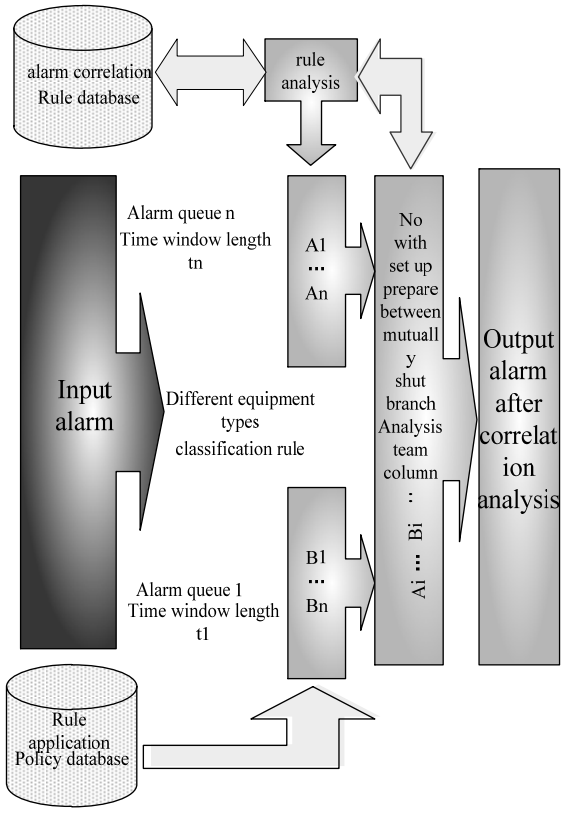

Figure 3. Analysis System Modular Diagram

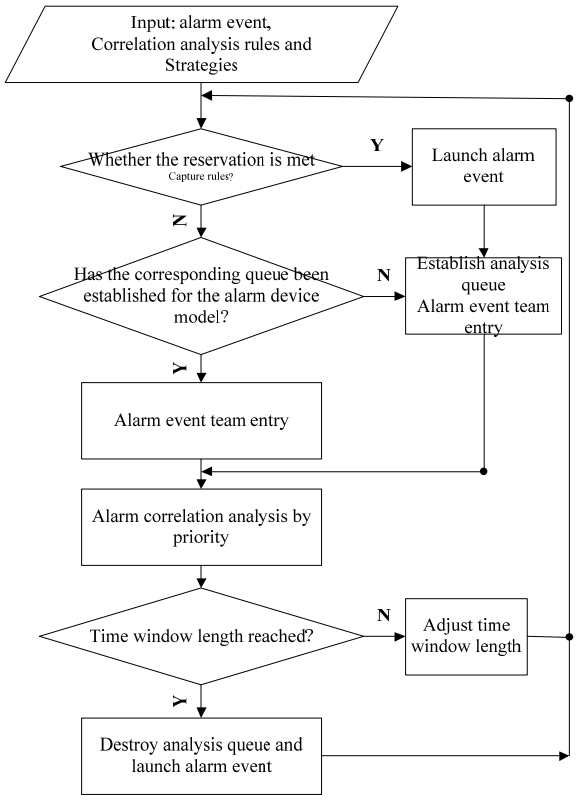

Figure 4. Analysis Flow Diagram

4.1. Principle of Correlation Analysis

As for the correlation characteristics, the alarm events belonging to the same area, the same equipment, the same system, the same time and other conditions have a larger correlation, while the alarm events belonging to different areas, equipment, systems, time and other conditions have a smaller correlation, or even no correlation shown in Figure 3.

Therefore, it is considered to divide all alarms into several correlation analysis processing queues according to the alarm correlation degree. Each queue has the maximum correlation according to the

conditions such as area, equipment, system and time. The correlation analysis is carried out for each queue respectively to filter out the same origin, related repeated, secondary and false alarms and get the root alarm group of each queue. Then, according to the correlation level, the remaining alarms in each queue are analyzed or output directly. In this way, a large number of alarm analysis without correlation between them is avoided, and the efficiency and processing speed of fault analysis are improved.

4.2. Analysis Process

The flow chart of alarm correlation analysis is shown in Figure 4.

The specific steps are as follows:

(1) step 1: when there is an alarm input, judge whether the queue of the device type of the alarm exists. If not, establish the alarm queue for the device type. Otherwise, the alarm event will be transferred to the team.

(2) step 2: read in the priority and time window length of the correlation processing type from the rule application strategy data table, and read in the rules belonging to the corresponding equipment model of the alarm from the rule data table.

(3) the third step: according to the priority of the correlation processing type, we call the correlation analysis interface and analyze it. Step 4: judge whether the queue has reached the time window length. If so, output all alarms in the queue, destroy the queue, transfer to the start, or transfer to the start, and adjust the window length.

5. Conclusion

Through the realization of the function of this article, it can quickly filter from many complex alarms in the power communication network, and finally determine the root cause of the fault, so as to shorten the decision-making time of fault processing, and improve the intelligent level of the operation and dispatching command of the power communication network.

According to the statistical analysis, the accident probability of electric power communication network is 0.05 times / year. In one year, the average maximum load of a province's power grid is 25 million kilowatts, and the average loss rate of load caused by communication fault affecting the important business of the power grid is 1%. Due to the function realization and practical application of this article in the intelligent analysis and decision-making system for operation and dispatching of electric power communication network, the fault processing time is shortened by 240 hours / year as a whole, and the multi transmission power is 300 million kwh. According to 0.45 yuan / kWh, the new output value is 27 million yuan / year.

6. References

[1] Zheng Qing-guo, Lv Wei-feng. The Alarm Correlation Analysis in Communication Network Management. Computer Engineering and Applications, 2002, 2:11-14

[2] WU Jian, Li Xing-ming. Efficient Distributed Mining Algorithm for Alarm Correlation in Communication Networks. Computer Science, 2009, 36(11):204-212

[3] Lu Xiaobin. Alerts correlation based on intrusion action pattern[J].Microelectronics & Computer, 2005, 24(7):17-20

[4] Li Mingfang. Relativity analysis of optical transmission network alarm based onignal flow[J].Telecommunications Technology, 2005, 22(10):23-26

[5] XU Peng, LU Hai-jun, LI Ming-wei. Alarm Filtering Mechanism for Power Communication Network Based on Event-Tree Model. Power System Technology, 2008, 32(8), 91-94.

[6] SHI Yong-ge, MEI Yu-jie, SHI Feng. Research and application of alarm filtering in network management systems. Computer Engineering and Design, 2008, 29(9):2169-2171.

[7] ZHANG Xian-fei, XU Run-ping, LI Shu-jing. Design of alarms stratification filtering mechanisms in power communication network. International Electronic Elements, 2008, 12:47-48.

[8] WANG Bao-yi, GUO Ya-wei, SHI Zhan-cheng, et al. Research of alarm correlation method based on dependency search tree in electric power communication network. Relay, 2008, 36(6):59-64.