An Alarm Correlation Model for Effective Network Management System: The case of ethio telecom National Network Operation Centre

Eskedar Derara
HiLCoE, Software Engineering Programme, Ethiopia
eskedarderara52@gmail.com

Taye Abdulkadir
HiLCoE, Ethiopia
tabdulkadir@gmail.com

Abstract

In most telecommunication networks, the existence of large number of network elements and associated fault alarms has burdened network management. As networks grow and network elements become heterogeneous, it creates a bottleneck at network operation centers in the management of the significant amounts of alarms and the resolution of associated faults. Moreover, a considerable part of fault alarms is not important or necessary for the fault isolation process. Correlating these different alarms and identifying their root cause is a major problem in fault management. Significant research has been done on telecommunication network operation centers in order to improve the performance of network management systems. However, correlating different alarms to improve the ease and simplicity on managing them is a less researched area.

This paper provides a comprehensive comparative analysis of existing alarm correlation approaches based on pre-selected performance metrics (parameters), covering two important areas: *availability* and *reliability*. In addition, a comprehensive assessment of the existing alarm management scheme at ethio telecom National Network Operation Center (NNOC) has been conducted based on similar metrics.

The outcomes of the comparative analysis and the NNOC assessment are used to propose an Integrated Alarm Correlation Model for ethio telecom NNOC to correlate large number of fault alarms to small number of root causes. An evaluation of the proposed model using real time data from the NNOC is also presented.

The result of the research verifies the advantages of the proposed Alarm Correlation model using the pre-defined metrics used. The total number of incoming active alarms for processing was 38,000 using manual and rule based filtering by identification of false alarms and unimportant alarms, we have identified and reduced the number to 993 total active alarms.

Keywords: Alarm; Alarm Correlation; Mean Time Between Failure; Mean Time To Repair; Case-based Event Correlation; Rule-based Event Correlation

1. Introduction

Telecommunication is the blood flow of modern economies which intensifies the productivity level that will in return make contribution towards the various important economic factors [1]. Ethio telecom is the sole telecom operator in Ethiopia owned by the Ethiopian government and exclusively provides overall telecommunication services including fixed, mobile, Internet and data communications. To centrally manage all these networks in one place, ethio telecom established the NNOC. NNOC handles large networks with a mix of legacy and new equipment and often this may lead to numerous alarms that make it difficult for network analysts to classify and prioritize troubleshooting.

Correlating the different alarms and identifying the root causes is the main challenge in the NNOC. Alarm Correlation is one of the ways considered in helping to understand problems through correlation and identifying root causes so as to apply solutions on a timely basis.

This paper provides an insight to the concept of alarm correlation in the context of ethio telecom NNOC and proposes a solution that alleviates the existing problem.

We used design science methodology using both qualitative and quantitative data. Qualitative data was gathered through interviews, observations, and document reviews. Quantitative data was gathered from statistical data collected from real-time network alarm flow.

The primary data gathered from the Element Management System (EMS) of ethio telecom NNOC was used for evaluating the alarm correlation model that is proposed in this paper.

A comparative analysis of existing alarm correlation approaches was conducted through comprehensive literature surveys. This covers Rule based, Case based, Data Mining based, and Codebook based approaches using the four metrics measuring *availability* namely, Mean Time to Repair (MTTR), Fault Isolation, Fault Localization, Actual Repair and the one metric measuring *reliability* - Mean time Between Failures (MTBF).

In addition, a comprehensive assessment of the existing alarm management scheme at ethio telecom NNOC was conducted based on similar metrics and findings are presented. These two aspects of the study help in proposing an alarm correlation model that best fits the needs of ethio telecom. Primary data collected at the IP unit of NNOC for one day has been used to evaluate the proposed model.

2. Literature Review

Alarms are short messages or notifications generated by a system component to indicate any abnormal condition. In other words, alarms are external manifestations of faults. They are defined by network operators and generated by devices in the event of a failure in a network. Alarms are commonly generated when a predefined threshold value is exceeded [2].

A single fault in a telecommunication network frequently results in a number of alarms being reported to the network operator. This multitude of alarms can easily obscure the real cause of the fault. Alarm correlation is a useful method and tool for analyzing alarms and finding the root cause of faults in telecommunication networks. In particular, the area of fault management remains a key problem which is difficult to identify and predict the root causes in a short period of time for network operators. The incoming rate of network alarms often becomes too high for a network operator so that the operator may not have enough time to recognize the network state without alarm correlation. The purpose of alarm correlation is to reduce the number of alarms and identify the root cause from the reduced set of alarms [3, 4].

There have been lots of research concerning the definition of alarm and alarm type concepts [5, 6, 7]. In general, most of the studies published and shared in this area assume a specific fault and use a single type of alarm correlation approach.

Case based alarm correlation is a method to solve problems using the experience of past cases. In this approach, problems are solved by the stored solutions. When a problem is solved, this solution is stored to be used in the future [8].

In *Rule based* alarm correlation, a specific rule is created to process each of the events. In this approach, sets of rules are matched to events when they occur [9].

Codebook based alarm correlation uses representation of relationship between problems and symptoms as a matrix. It encodes the relationship between network faults and their symptoms by creating a matrix of problem codes that represent the dependency between the symptoms and the problems [10].

Data Mining based alarm correlation is used to detect the frequent event sets and identifies a root cause among the collected alarms. In this approach, frequent event sets can be detected by several mining algorithms [11].

There are some works on quality of alarm management. But there is a lack of detailed analysis on proposing an integrated alarm correlation approach. This paper focuses on selecting an alarm correlation approach that best suites the case of ethio telecom NNOC.

3. Comparative Analysis of Alarm Correlation Approaches

A comprehensive comparative analysis of selected alarm correlation approaches has been conducted through the review of literature. The basis of comparison was the metrics measuring availability and reliability. The comparative analysis was conducted through a detailed desk research about the selected alarm correlation approaches namely, Case Based, Rule based, Mining based and Codebook based using the selected metrics for the research.

Availability metrics is assessed by MTTR using Fault Isolation, Fault Localization and Actual Repair. *Reliability* metrics is assessed by MTBF.

The comparative analysis assesses the advantages and disadvantages of each alarm handling method. The conclusion based on the comparative analysis is that a combination of Case based and Rule based approaches provides better performance in comparison with the other approaches.

Some of the leading guides to make the conclusion are discussed below:

- *Codebook Based Approach*: The dependencies between observable causes and underlying problems are examined and suitable subset of the symptom of the alarm is selected referring to the codebook. In such kind of problem, the codebook must be large to identify the root cause of the problem. When the codebook is large it provides redundancy. It is not possible to know the cause of a specific problem and doing it manually is not possible and has effect on time of fault localization.
- *Data Mining or Association Based Approach*: This process can take many steps to localize network faults such as alarm filtering and correlation of network faults. This step requires large processing capacity. It has complex design and resource requirements that lead to consume much system resources (CPU and memory).
- *Case based* and *rule based* alarm correlation approaches are active in the sense that they do not start their fault analysis process until they receive malfunctioning indications from the managed network. Hence, they do not induce extra management traffic. This of course implies that they may not be able to anticipate network failures in advance.
- *Case based* and *Rule based* alarm correlations are extremely easy in isolation of network faults. Therefore, as per the predefined metrics, we chose case based and rule based alarm correlation approaches.

4. Findings from ethio telecom NNOC Assessment

The basis for the NNOC demand is a centralized network resource management which will also contribute to an efficient network planning. There are basic systems that are used in monitoring of network devices in NNOC such as Element Management System (EMS), Fault Management System (FMS), and Trouble Ticket System (TTS).

Currently, NNOC deployed no mechanisms to improve the traditional ways used for locating and maintaining network faults. Due to this, it is not able to ensure or increase customers' experience on service quality and there is a limitation on operational readiness to market new services.

The existing alarm management at NNOC was assessed using qualitative and quantitative data collected through interviews, document reviews and observations. Out of the six units in NNOC, the IP technology unit was selected for the research. As all the other units follow the same approach in managing faults, the outcome from this unit will be representative to all other units. Despite the challenges on timely response and density of respondents, the research managed to arrive at concrete findings and conclusions that highlight the working challenges at NNOC, including:

- Many network events triggered by a fault are typically generated within a short time window, which result in difficulty of network fault isolation and localization.
- For every new network alarm coming to the network management system, irrelevant network alarms are also considered, due to the absence of alarm correlation.
- Massive individual network alarms result in difficulty of the actual failure or inferring of the root cause reasoning capability of network analyst teams.

5. The Proposed Solution

Figure 1 depicts the proposed comprehensive model for NNOC alarm correlation.

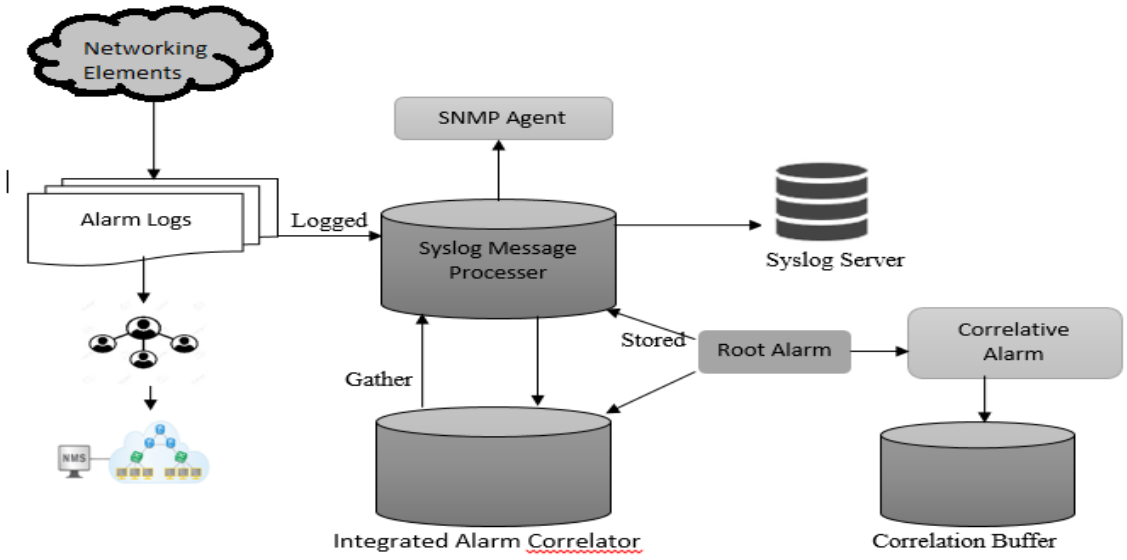

Figure 1: Alarm Correlator Model for ethio telecom NNOC

The comparative analysis of alarm correlation approaches and the assessment of the existing system at ethio telecom provided the necessary input to decide on an integrated alarm correlation approach that combines *rule based* and *case based* approaches. The proposed model also describes the concepts and tasks related to alarm log information and correlated alarm records. Syslog message processor extends the model to include the ability to group and filter messages generated by various network devices and helps to isolate root alarm messages from correlated alarms. The components of the proposed alarm correlation model, as shown in Figure 1, are described below.

- *Alarm Log:* The alarm logger is the final destination for system logging messages forwarded on the router. It stores alarm messages in the logging events buffer. The logging events buffer is circular, that is, when full, it overwrites the oldest messages in the buffer.
- *Integrated Alarm Correlator:* It filters, aggregates, and correlates alarms from different sources. The correlator receives messages from Syslog message processor that are distributed across the nodes on the network element and forwards Syslog messages to the Syslog server. The correlator continues searching for a match to messages in the rule until it gets the root alarm. If the root alarm message was received, then correlation occurs; otherwise, all captured messages are forwarded to the Syslog message processor. When a correlation occurs, the correlated messages are stored in the correlation buffer database and the correlator tags each set of correlated message with a correlation ID to identify from other messages. From the Syslog Message processor, the identified root messages are sent to the final destination such as NNOC Network Management System and SNMP agent. The network analyst is able to retrieve all the correlated messages from the already logged database.
- *SNMP Agent:* Operates on the managed device. The agent is implemented to send traps on different events. It also responds to requests from NMS. The implementation of an agent is based upon Management Information Base (MIB) files.
- *Syslog Server:* Logging correlation can be used to isolate the most significant root messages for events affecting system performance. A network operator can retrieve all correlated messages from the logging

correlation buffer to view correlation events that have occurred.

Network management system consists of monitoring data and alarm messages from the network devices. To understand the causes of these received data, the data must be processed. Processing the network monitoring alarm information is referred to as correlating the alarm. To correlate the monitoring alarm information, it is required to determine what alarm information is important, which network alarms are related to each other, and which alarm indicates the real cause for a network problem. These correlation rules are either defined by network experts (using case based) or generated automatically after discovering the correlation rules by an integrated alarm correlation model.

6. Implementation and Evaluation

The proposed integrated alarm correlator is modelled by a knowledge base (correlation rules) which is formulated using PL/SQL. The targeted network components constitute the initial domain knowledge obtained from NNOC network experts through a series of interviews.

In order to show the improvement on alarm management after the implementation of the proposed model, we used real time data. The data was gathered from IP network by U2000 EMS. Network elements from Huawei were chosen to cover a large number of monitoring areas than Ericsson and ZTE vendors. IP network is managed by U2000 (U stands for unified) EMS. Studying the event logs of U2000, we found that the most common fault types in this network were due to Equipment, Process, Communication, Service, and Environment. Network Analysts often need to read through hundreds of event messages to identify the problems, which in most cases, are only a few.

To evaluate the practicality of the proposed approach, Oracle Minor by PL/SQL was used, to correlate events generated from real networks. In order to evaluate the proposed alarm correlation model, we started by analyzing the real alarm data samples from live IP Huawei network containing different network elements. We looked larger active alarm data sets that were available on the fault management system. The second data set contains 2,620 alarm details. Both are presented below.

a. *Active Alarm Data Sets:* Real IP active alarm data from U2000 EMS was collected and analyzed with a total of 38,000 network alarms having false and true alarms. The main types of information provided are Severity, Device Name, Alarm Name, and Parent Alarm. False alarms are alarms triggered by the fault management system when it should not have, for instance, alarms triggered in a healthy network.
b. *Detail (distinct) Alarm Data Sets*: Real IP detail alarm data sets from U2000 EMS was collected and analyzed by gathering a total of 2,785 network alarms which are distinct alarms categorized under five parent alarms (Equipment, Process, Communication, Service, and Environment) for the IP technology unit. The main types of information provided are Alarm Name and Parent.

The data set we used to test the result of manual filtering and rule based filtering were done using active and detail alarm data sets.

- *Manual Filtering:* There were a total of 38,000 active alarms collected from the EMS. But a total of 6,238 alarms were manually eliminated with no alarm information and with warning severity (only critical and major alarms were used). No alarms related to warning severity and alarms with no valuable information were ignored. Only 31,762 active alarms were identified and considered as important alarms.
- *Rule Based Filtering:* One important challenge we faced when using this alarm data set is lack of real alarms that were indications of false and true alarms. The identification of true and false alarms is used for NNOC in order to effectively prioritize alarms. This is especially helpful in the case of large events, which generate important alarm messages that need to be processed fast.

a. Results for Distinct IP Alarm Data Set

From 16 fault types, only five fault types are selected. The parent Alarm is classified under five fault types: Communication, Environment,

Equipment, Process, and Service. Then the alarm rule based filtering on detail alarms was done to classify and identify each alarm type under a specific parent alarm category. The accuracy of each parent alarm classification is calculated as:

$$\text{Accuracy} = \frac{\text{Number of correctly classified}}{\text{Total number of Parent Alarms}}$$

Table 1 shows the results of the rule based filtering in terms of accuracy on the test data sets. As the last column indicates, the method is likely to classify the alarms into parent alarms with a very high accuracy.

Table 1: The Accuracy of Detail Alarm Data Set Classification

Parent Alarm	*Total*	*Correct Classification*	*Incorrect Classification*	*Accuracy*
Communication	470	432	38	0.91
Process	900	876	24	0.97
Environment	238	221	17	0.92
Service	245	210	35	0.85
Equipment	932	881	11	0.94
Total	*2785*	*2620*	*165*	

b. Results for Active Alarm Data sets

All active alarms which occur less than four and greater than 250 times are considered as false alarms in the proposed database because those alarms are categorized under intermittent alarms (frequently repeated alarms) which have lower impact. We considered the frequency of the alarm occurrence as threshold. The higher the probability the alarm was false or the device was intermittently down. The dataset (generated by artificially increasing failure rates) includes event bursts of sizes up to 31,762 alarms. In total, 31,762 active alarms were recorded, out of which 11,273 (35%) were false alarms which were eliminated using the rule based filtering. But clearly from the total of 31,762 active alarms, using rule based filtering process, we identified 20,489 total active alarms. Obviously, it is desirable to be able to suppress these repetitive and redundant alarms such that at most one alarm message, corresponding to one fault, is sent to the network analyst team.

Filtration of true and false alarms on active alarm data set is done since not all incoming alarms are relevant for further processing. However, after identifying true active alarms, it is necessary to judge which alarm is relevant for future and which is not.

c. Results of the Alarm Correlation

Mapping is done for each 2,620 detail alarm data sets and 20,489 active alarm data sets were identified under common parent alarms Communication, Equipment, Process, Service, and Environment. From active alarm and alarm detail, each alarm name is grouped by parent alarm and device name.

The Efficiency of the proposed alarm correlation (X) is calculated as:

$$X = \frac{\text{Total active alarms - Correlated Alarms}}{\text{Total active alarms}} * 100$$

$$X = \frac{20{,}489 - 993}{20{,}489} * 100$$

$$= 0.95\%$$

Using manual filtering, Rule based filtering and correlation the analysis of the number of total active alarms becomes 993. It has been proven that alarm correlation can significantly reduce the size and the quantity of the network alarm data analyzed which makes the network analysis process or troubleshooting of faults much faster and more efficient. The results indicate that it is possible to set optimal alarm information generated by the fault management system using alarm correlation model. This helps to identify network faults at faster rate, indicating a shorter recovery time compared to the current alarm management. As a result, we were able to reduce the number of alarms from 20,489 to 993. Network analysts can now quickly find the problems and fix them. It also becomes easier to categorize each alarm into its fault type.

Figure 2 summarizes the evaluation of the proposed alarm correlation model based on the data set taken from real NMS of IP technology unit.

The proposed network alarm correlation model has the potential while maintaining all the required functions.

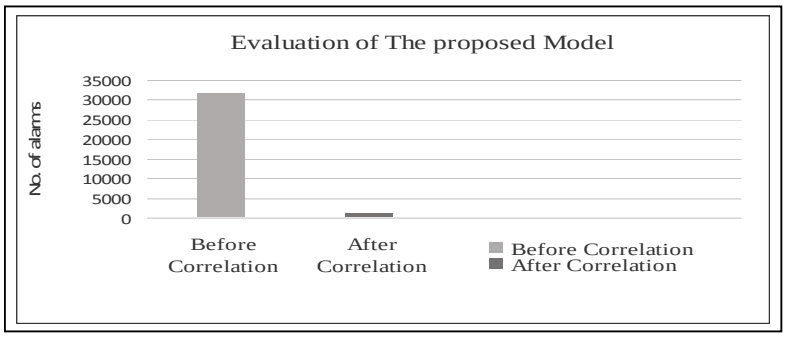

Figure 2: Evaluation of the Proposed Model

7. Conclusion and Future Works

This paper provides an insight on the different alarm correlation approaches, assessed the management of network alarm and proposed a solution in order to address the challenges of the current alarm management. The proposed alarm correlation model makes an effort to optimize the advantages provided by case based and rule based approaches. An integrated alarm correlation model strengthens the advantages of these two approaches.

Integrated Alarm Correlation Model is recommended to be used in telecom operators' network operation center and its final goal is improved network problem detection leading to better reaction to problems. In that case, network users will not perceive existing network problems as service degradation.

The proposed alarm correlation model processes the incoming alarm information and determines the faults from the alarms. It attempts to narrow down the likely root causes of each fault, to the greatest extent possible, given the available information.

As future work, we are investigating versions of an integrated alarm correlation model that are able to improve the ability of the model to predict failure conditions of network elements and enhance its capability to recognize any network topology changes.

References

[1] Karimganj, Assam, "Telecommunication and its Impact over the Economic Development of SAARC Countries", International Research Journal of Interdisciplinary & Multidisciplinary Studies (IRJIMS), 2017.

[2] Sunthari Solaimalai, "Intelligent Fault Management using Cost Sensitive Fault Remedial Approach", 2011.

[3] A. S. Sethi, Y. Raynaud, and F. Faure Vincent, "Integrated Network Management", 1995.

[4] Li Jing-hua and XU Gung-hui, "A New Network Management Framework Design and Application Realization", Proceedings of the Sixth International Conference on Parallel and Distributed Computing, Applications, and Technologies, IEEE Computer Society, 2005.

[5] R. Gardner and D. Harle, "Alarm Correlation and Network Fault Resolution using Kohonen Self-Organizing Map", Globecom 97 Proceedings, pp. 1398-1402, 1997.

[6] Chen, S-K., Jeng, J-J, and Chang, H, "Complex Event Processing using Simple Rule-Based Event Correlation Engines for Business Performance Management", Proceedings of the Int. Conference on E-Commerce Technology and E-Services, 2006.

[7] Y. Tan, X. Gu, and H. Wang, "Adaptive System Anomaly Prediction for Large-Scale Hosting Infrastructures", In Proceedings of the 29th ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing, 2010.

[8] L. Lewis, "A Case-Based Reasoning Approach to the Management of Faults in Communications Networks", In Proc. IEEEINFOCOM, pp. 1422-1429, 1993.

[9] W. Fuller, "Network Management using Expert Diagnostics", International Journal of Network Management, pp. 199-208, 1999.

[10] Minaxi Gupta and Mani Subramanian, "Pre-processor Algorithm for Network Management Codebook", 1999.

[11] Ann Devitt and Joseph Duffin Rober, "Topographical Proximity for Mining Network Alarm Data", 2005.