Advanced Correlation Engine for Fault Identification and Analysis in Network

Preethi D’Souza
M.Tech, Computer Network Engineering
BMS College of Engineering
Bangalore, India
dsouzapreethi@gmail.com

M.Dakshayini
Professor (ISE)
BMS College of Engineering
Bangalore, India
dakshayini.ise@bmsce.ac.in

Abstract

With the growing complexity of modern communication systems one of the key challenges for telecom service providers is to provide operations support system (OSS) that enable rapid deployment of new services, thereby fulfilling quality of service (QoS) requirements as prescribed by Service Level Agreement (SLA’s). Occurrence of single fault or invalidation in network leads to alarm floods and deducing the exact source of a failure is very challenging. The existing alarm correlation approaches still rely on the manual processing, and depend on the knowledge of the network operators. This paper discusses about various approaches used in fault localization and proposes automated alarm correlation approach to filter out redundant and spurious events and determine the root cause of faults in a network. The proposed technique performs well in terms of efficiency and accuracy of identifying root cause thereby improving the service quality and reliability.

Keywords – events, correlation, fault localization

1. Introduction

The network management is the collection of tasks performed to maximize availability, performance, security and control of a network and its resources. The International Organization for Standardization (ISO), Network Management Forum has divided network management into five functional areas. They are Fault Management, Configuration Management, Performance Management, Accounting Management and Security Management. Fig 1.1 depicts the functional areas of network management system popularly as FCAPS model.

Typical Fault management functionalities include:

- Monitoring and collect of statistics on network devices, traffic conditions and usage in real-time to avoid and forecast potential faults.
- Setting thresholds and alarms that may cause network failure to warn the network admin.
- Setting alarms that warns of performance degradation on network devices and links.
- Setting alarms of network resource (such as hard disk space) usage and limitation problems.
- Remotely control network devices for rebooting, shutting down etc.

Fig 1.1 FCAPS model
Network Operation, Administration and Maintenance (OAM) are very crucial for efficient operation. Telecom careers are expected to ensure SLA and must compensate a customer on its violation. Thus, service provider keeps track of service qualities and identifies the sign of a problem up front to meet SLA. An efficient network fault management must be able to perform consistently well in all types and sizes of networks. With the wider classification of network services and technologies management of network generated alarms and the time to identify the root cause of a failure has increased significantly resulting in degradation of service qualities.

Network elements report about their state in the form of alarms in timely manner. These alarms can be either good which indicates the health or may be the ones which indicate abnormal network conditions. Hence it becomes a huge task for a network manager to manually sit and analyze each of these alarms, segregate them based on their conditions and take necessary actions in case of fault. For time critical systems it is required that system must be up and running 24*7. Customer satisfaction solely depends on building robust and fault tolerant systems.

Traditionally, fault localization has been performed manually by an expert or a group of experts experienced in managing communication networks based on network disorder symptoms displayed on a management console. Fig 2.1 depicts the view of network operations with and without integrated Fault Manager. With automated FM system we can integrate and monitor multiple technologies from multiple vendors with limited human resource.

2. Fault Management Terminologies

Event is an exceptional condition occurring in the operation of the hardware or software of the managed network.

A fault is an event that is associated with an abnormal network state, i.e., network behavior that deviates from expectation. This deviation can be attributed to hardware/software failures, human errors, design flaws, or a combination of the above. Network faults can be classified as being hard or soft. A hard fault occurs when managed objects fail completely (e.g., a router link failure, link cut, or a server crash); a soft fault occurs when managed objects function in a degraded performance state. In general, a soft fault may cause a hard fault, and vice versa.

Symptoms of network faults are observed as alarms – notifications of a potential failure which originate from management agents via probes. Event correlation works by establishing relationships between network events. We say that an event $e$ correlates a set of events $e_1, e_2, \ldots, e_k$ written as $d(e_1, e_2, \ldots, e_k)$, if $e_1, e_2, \ldots, e_k$ by entering into a relationship with each other and with $e$ define the event pattern $e$.

3. Related Work

Fault localization techniques are broadly classified as below and some of the techniques are elaborated in detail in this section.

- model-based reasoning tools
- fault propagation models
- model traversing techniques
- case-based reasoning tool

Finite State Machine Based: This techniques works by constructing FSM based event correlation model which is used in fault identification. Error will be reported whenever an event occurs leading to invalid state. Multiple event patterns can be modeled individually and combination of all models can be used to monitor a complete system.

Rule Based Event Correlation: Rule based reasoning is one of the most popularly used. It consists of three levels:

- Data level {working memory or global database, which contains information about the problem at hand.
- Knowledge level {a knowledge base (rule repository), which contains domain-specific expert knowledge.
- Control level {an inference engine, which determines how to apply the rules from the knowledge base to solve a given problem.

Practical implementations of rule based approach work on RETE algorithm and its variants. One of major concern is to update the rule base continuously updated to handle evolving alarm list.
Case Based Reasoning: In Case-based Reasoning (CBR), each new problem in hand is compared with that present in case library and if matched solution is applied. If the match is not exact then the solution is adapted according to current problem and also a copy is saved in case library.

The advantage of this approach is that knowledge from past cases can be reused automatically with expansion of knowledge base with each solved problem. This helps in user acceptance of system with learnt decisions. Retrieval of similar cases from case library and its adaption is quite challenging. Practical implementations include CRITTER, CHEF program, Compaq's Support Management Automated Reasoning Technology (SMART).

Model Based Reasoning: The basic idea of Model-based Reasoning (MBR) consists of description of the structure, a description of the behavior and a set of guidelines to investigate misbehavior based on these two descriptions. In contrary to a rule-based correlation engine, which specifies event patterns as conditions for certain actions, an MBR system specifies a system model, with events as consequences of certain model states or transitions. In a computer network, the application of MBR methods may be unsuitable, as the description of the network structure and the behavior of each service would likely be too difficult and time consuming.

Codebook Based Event Correlation: Here the dependencies between observable symptoms and problems are examined and a suitable subset of the symptom events is selected to form codebook. A binary vector for each problem is then created, which indicates, whether each symptom in the codebook can be caused by that specific problem. It works based on Hamming distance and comparatively a faster approach. Additionally, there is a good tolerance to lost events or noise.

Explicit Fault-localization: In explicit fault localization, information is associated with each alarm. With reliable alarm set and with only a single fault in the network, fault lies in the intersection. Alarms that share a common intersection location should be correlated.

Practical implementation needs priory information and a method to gather it automatically. It works well with single faults in network which is not very realistic hence, extension to cover multiple faults is proposed by authors.

Dependency Graphs: In dependency graph, dependency between network elements is modeled as a directed graph where nodes represent network elements and edge denotes the dependency relationship. An edge from node A to node B indicates that failures in node A can cause failures in node B. The main objective is to get root cause from the relationship details.

Bayesian Network Based Event Correlation: The key principle in Bayesian Network is probabilistic theory. It's being modeled as a directed acyclic graph of network elements, represented by random variables. This technique requires historical data and expert knowledge for the smooth functioning.

Neural Network Approach: An ANN is a network of processing nodes which perform operations on the weighted inputs to generate an output. The computations vary from simple mathematical operations, to more complexes which involve temporal operation or memory parameter evaluations. Dynamic adaptation of input weight is carried out to facilitate automatic learning.

4. Proposed System

Two major approaches that are followed over the recent years to implement RCA include rule-based approach which identifies the root cause based on event correlation rules which are defined in advance. The other is a dependency graph based RCA approach which identifies the root-cause using the relationship based on network topology information.

**Fig. 4.1 Data Flow of Hybrid Approach**

Rule based correlation techniques use flavors of RETE algorithm which is already proven faster and effective and emerge as one of the widely used techniques. In a rule based system the knowledge level consists of rules with condition-action specifications. Each rule describes the action need to be taken when a specific condition occurs. Data level consists of run time network conditions on which rules will be acted upon. Finally inference engine applies rules on the working data and gives out the result. Along with the inbuilt
capability of quickness of RETE this also needs a strong network knowledge gained over the years by network operators to know network patterns to build strong rule set that capture most of fault causing conditions and identify the root cause. Making this practically possible is quiet challenging with growing network size, complexity and types of network elements in place.

In dependency graph based solutions the relationship among various network components is depicted using directed graphs and cause is identified by backtracking through the relations. The dependency view helps in identifying the actual issue thereby isolating and filtering the root cause among others quickly as possible. This technique being more generic can be applied as long as network hierarchy is known pre-hand.

The hybrid approach combines the ideas of these rule based as well as dependency graph techniques to build an automated and robust fault management system. The input alarms generated from various network elements are collected and normalized. The dependency graph is formed out of the alarms and root cause is identified based on the hierarchical dependency. The first level results are then passed through the rule based event correlation channel. The resultant alarm set is greatly reduced and displayed on the management console of the network operators. Network operator then takes appropriate action on the alarms to either run automated commands to fix the failures or to raise a manual trouble ticket which needs personnel to manually trouble shoot the problem.

The rule-based approach needs a high expertise in network conditions and is written in high-level policy language. In contrast, the model-based approach is easy to deploy and modify and is appropriate for a large-scale network if the network resource information is available.

5. Conclusion

This paper mainly focuses on various event correlation techniques which are in use today. Based on the practical usage each technique has been employed in various aspects of computer networks domain. With the growing and complex systems developing a robust correlation technique is quite challenging.

The proposed system makes an effort to optimize the advantages provided by rule based and dependency graph correlation systems to build a highly robust and faster system to detect faults and to take appropriate diagnostic measures on the network recovery.

6. References


[6] Nahid Amani, Mahmood Fathi and Mehdi Dehghan,” A Case-Based Reasoning Method For Alarm Filtering And Correlation In Telecommunication Networks”, IEEE CCECE/CCGIEI, Saskatoon, May 2005


