OPERATIONS SUPPORT SYSTEMS, IMPLICATION OF SOFTWARE ERRORS IN GSM NETWORK PERFORMANCE (A CASE STUDY OF Airtel NETWORK)

BY

OTORI, ABDULAZIZ UYE

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
AHMADU BELLO UNIVERSITY, ZARIA
NIGERIA

MARCH, 2012

OPERATIONS SUPPORT SYSTEMS, IMPLICATION OF SOFTWARE ERRORS IN GSM NETWORK PERFORMANCE (A CASE STUDY OF Airtel NETWORK)

BY

OTORI, ABDULAZIZ UYE
MSC/ENG/10508/2007-08

A THESIS SUBMITTED TO THE SCHOOL OF POSTGRADUATE STUDIES, AHMADU BELLO UNIVERSITY, ZARIA IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE (M.Sc) DEGREE IN ELECTRICAL AND COMPUTER ENGINEERING

MARCH, 2012

DECLARATION

I declare that the work in this thesis entitled: "OPERATIONS SUPPORT SYSTEMS, IMPLICATION OF SOFTWARE ERRORS IN GSM NETWORK PERFORMANCE: A Case Study of AIRTEL Networks, Nigeria"; has been done by me in the Department of Electrical Engineering, Faculty of Engineering, Ahmadu Bello University, Zaria under the supervision of Dr. D. D. Dajab. The information derived from the literature has been duly acknowledged in the text and in the list of references provided. No part of this thesis was previously presented for another degree or diploma at any university.

_____ _____

OTORI, Abdulaziz Uye Date

CERTIFICATION

This thesis entitled: "OPERATIONS SUPPORT SYSTEMS, IMPLICATION OF SOFTWARE ERRORS IN GSM NETWORK PERFORMANCE: A Case Study of AIRTEL Networks, Nigeria" by OTORI, Abdulaziz Uye meets the partial requirements for the award of Masters of Science degree in Electrical Engineering in the Department of Electrical Engineering, Faculty of Engineering, Ahmadu Bello University, Zaria and is examined and approved for its contribution to knowledge and literary presentation.

_____ _____

Dr. D. D. Dajab — Date
(Major Supervisor)

_____ _____

Dr. M. B. Muazu — Date
(Minor Supervisor)

_____ _____

Dr. M. B. Muazu — Date
(Head of Department)

_____ _____

Prof. A. A. Joshua — Date
(Dean, Postgraduate School)

DEDICATION

This work is first dedicated to Almighty GOD, whose divine guidance and unmistakable lead guided me during the research work and to: my beloved wife, Bonita; our treasured Stephanie; Christabel and Samuel-Great.

ACKNOWLEDGEMENTS

I appreciate my amiable supervisors, lecturers and fellow colleagues for the support and assistance they rendered to me. Every kind of assistance that made this research a success is deeply appreciated. Hence, My thanks goes to: Dr. D. D. Dajab, Dr. M. A. Muazu, Prof. B. G. Bajoga, Dr. J. Y. Oricha, Dr. J. Boyi, Dr. B. A. Adegboye, E. O. Adetiba, Martins, Engr. Akinsanmi, Pastor W. Adedokun, Pastor (Prof.) J. A. Onaolapo, John, H. M., Engr. J. O. Ikhigbonoaremen, Engr. Kazeem (Airtel Networks), Pastor Nathaniel Osigbene, Raphael Udoh, Engr. Suleiman Garba, Engr AbdulFarouk Aguye, Engr. Shaban, Engr Gbenga, Engr Kabiru, Engr. Sikiru, Mr Wahab Jimoh, Beky, Mr. Saliu Omeiza, Mrs. Oyeleye (Airtel Networks), Engr Jide Omotowa, Engr. Shittu Ahmed, Dr. Solomon Avidime, Prof. Lawal Idris, Architect Ozovehe Saliu, Mr. Maxwel,Engr. Fatai, Engr. Dr. & Mrs. Abejide and a host of friends too numerous to mention herein.

ABSTRACT

One of the most important requirements to be addressed by a general purpose Fault Management (FM) system is the ability to quickly identify the root cause of network errors and fix them as soon as possible. This informs the maintenance of an accurate model of the mobile network error logs for the FM task and the faults dynamic feature trend/statistical analysis of the error-log message summary for both the Base Station Subsystems and Mobile Switching Centers by comparing the relationship between the twin parameters of Frequency of Occurrence and the Mean Time to Repair each fault type. The Fault Trend Analysis shows that as the numbers of times a particular fault type occur increases the Mean Time to Repair such faults decreases, with some deviation from this trend in some cases when we classified them as high priority faults with serious impact on network performance and those that have little or no impact on network performance. Filtering and Correlation are two methods we used to simplify the separation of the principal alarms and redundant alarms from their side effect on network performance. These algorithms are also presented: Bayesian Inference Technique and Intelligent Management Information Base (I-MIB) MATLAB Simulation, which enabled us to systematically combine the qualitative and quantitative aspects of the Bayesian model for network fault management analysis and to reduce total computational complexity by providing a database of software alarm parameters respectively. These resulted in a Global Bayesian Network which helps to represent causal chains, i.e. links between cause/effect relationships to provide the evidence of past events and show the most likely future causes and their symptoms by computing Conditional Probabilities of each Symptoms given a particular cause i.e. using the expression $P(S= S_{i,j} / C= C_k)$ to populate the Conditional Probability Table. This is critical and useful for effective Global Systems for Mobile Communications/General Packet Radio Service (GSM/GPRS) Fault Management Systems and could be deployed by Service providers for quick and proper diagnosis/troubleshooting of network event/alarm error-logs to help reduce the total downtime and improved quality of service.

TABLE OF CONTENTS

Cover page…….…… i

Declaration…….…. ii

Certification ……..…… . . iii

Dedication……..…….…….…... iv

Acknowledgements..…….…….…...v

Abstract…….…...vi

Table of Contents …...…….…… vii

List of Tables …..…….…….…….……...x

List of Figures..…..……..…….…..... xiv

List of Appendices ...……...……... xix

List of Symbols and Abbreviations……....……..xx

Chapter One ….....1

Introduction……..…….……1

1.1

Preamble…….1

1.2 Thesis Motivation ….....4

1.3Statement of Problem ……..…….…….…..5

1.4 Thesis Outline…….....6

Chapter Two……...….7

Literature Review and Theoretical ackground…….…….…....7

2.1 Literature Review.....7

2.2 International Telecommunications Union FCAPS and OSS Framework…….... 10

2.2.1 Fault Management……..…….…….14

2.2.2. Sof tware Management ……..…….....15

2.3 Fault Diagnosis System Based on Bayesian Networks …….…….……...17

2.3.1 Bayes' Theorem …….……..…….….. 18

2.3.2 Bayesian Networks …….…….…19

2.4 Software Reliability Concept ……..…….. 21

2.5 Software Alarm Filtering and Correlation Technique ..…..……..…….24

2.5.1Rule-Based (Model-Based) System…….…….…….…….…….25

2.5.2 Codebook System……..…..……..…26

2.5.3 Artificial Intelligence Systems……..…..27

2.6 Integrated Diagnostic Techniques Based on Neuro-Fuzzy Inference AI System……...28

Chapter Three…..……....31

Design Methodology and Data Collection ……..……..…….…….31

3.1 Introduction…….……...….31

3.2 Methodology …….…….…31

3.3 Data Collection...…….……..32

3.4 Presentation of Derived Parameters (Data).....33

ChapterFour.....35

Results and Analysis.....35

4.1 Introduction.....35

4.2 Fault Trend Analysis of Network Elements Error-Log

Message Summary.....35

4.2.1Fault Trend Analysis of Base Station Subsystems (BSS) Error-Log message.....36

4.2.2 Fault Trend Analysis of Mobile Station Center (MSC) Error-Log Message Summar.....38

4.2.2.1Interpretation of Results for MSC.....39

4.3 Bayesian Modelling of BSS and MSC Derived Error-Log Message Summary.....40

4.3.1 Qualitative Modeling of Network Elements Error-Log Message Summary Using Simple Bayesian Model (SBM) (First phase).....41

4.3.2 Quantitative Modeling of Network Elements Error-Log Message Summary Using Bayesian Modelling (BM) (Second Phase).....43

4.3.2.1 Interpretation of Results.....46

4.4 Intelligent Management Information Base (IMIB) MATLAB Simulation for Bayesian Inference Using Visual Querry Builder GUI Database Tool (Proposed).....47

4.4.1 Setting Up a Data Source to Work With the VQB.....48

4.4.2 Interpretation of the Simulated Result.....50

ChapterFive.....54

Conclusions and Suggestions for Further Work.....54

5.1 Significance of the Study.....54

5.2 Limitations.....55

5.3 Summary.....56

5.4 Conclusions.....57

5.5 Recommendations for Further Work.....58

References.....60

Appendices.....66

LIST OF TABLES

Table 4.1: Table Showing MSC Classified High Level Priority Faults with Major Disturbance on the Network……..……
…38

Table 4.2: Table Showing MSC Classified High Level Priority Faults with little or no disturbance on the Network……..……39

LIST OF FIGURES

Figure 2.1: Mapping Between TMN Reference Model and FCAPS……12

Figure 2.2: GSM Network architecture and OSS……13

Figure 2.3: Alarm Mapping to Neural Networks……30

Figure 4.1: Area Chart Comparing Frequency of Occurrence and Duration for BSS Alarm Summary…….……..37

Figure 4.2: Area Chart Comparing Frequency of Occurrence and Duration for BSS Alarm Summary Comparing BSC High Level Priority Faults: (a) With Serious Impact on Network Performance and (b) With Little or no impact on Network Performance…….…….……..…37

Figure 4.3: Area Chart showing the relationship between Frequency and Duration of MSC High Level Priority Faults with major disturbance on network performance….38

Figure 4.4: Area Chart showing the relationship between Frequency and Duration of MSC High Level Priority Faults With Little or no impact on Network Performance …39

Figure 4.5: Simple Bayesian Model of BSS Faults (Error-Log Message) Summary…..41

Figure 4.6: Simple Bayesian Model of MSC Faults (Error-Log Message) Summary……..…42

Figure 4.7: Global Bayesian Network Model for BSS Error-Log Message Summary……...45

Figure 4.8: Global Bayesian Network Model for MSC Error-LogMessage Summary……45

Figure 4.9: Chart Showing the MATLAB Database ODBC/JDBC Connectivity with Directory of the Error-Log Summary……..…...48

Figure 4.10: Visual Querry Builder (VQB) window…….…….48

Figure 4.11: Create New Data Source Window……..…49

Figure 4.12: (a) Database Directory Path window (b) ODBC Workbook Excel Setup……..49

Figure 4.13: ODBC Data Source Administrator Window……...…….50

Figure 4.14: Visual Querry Builder Data Operation and Execution Pane. ……..51

Figure 4.15 Extracted Fields on Array Editor: ……...….…….52

LIST OF APPENDICES

Appendices……66

Appendix 1……..……66

Appendix 2……...……..70

Appendix 3……73

LIST OF SYMBOLS AND ABBREVIATIONS

SYMBOLS

$\prod$	N- Ary Product
μ	Micro Sign
λ	Lamda
$\sum$	N- Ary Summation
@	Commercial AT
{	Left Curly Bracket
}	Right Curly Bracket
$\approx$	Almost Equal To

ABBREVIATIONS

ANFPN	*Adaptive Neuro-Fuzzy Probabilistic Network*
BSS	*Base Station Subsystem*
COPEX	*Cost of Operation*
CPT	*Conditional Probability Table*
FCAPS	*Fault, Configuration, Accounting (Authentication), Performance & Security*
FCPN	*Fuzzy Causal Probabilistic Network*
FM	Fault Management
GUI	Graphic User Interface
IETF	Internet Engineering Task Force

I-MIB	*Intelligent Management Information Base*
ITU	*international Telecommunications Union*
MATLAB	Matrix Laboratory
MSC	*Mobile Switching Center*
OSS	*Operations Support Systems*
SLA	*Service Level Agreement*
SQL	*Structured Querry Language*
SOA	*Service Oriented Architecture*

CHAPTER ONE

INTRODUCTION

1.1 Preamble

The Second Generation Global System for Mobile communications (2G GSM) was designed primarily to provide circuit switched speech and data value added services were simply based on the Short Message Services (SMS). Today, most GSM network Operators are experienced in a voice oriented Time Division Multiplexed (TDM) technologies and have gone further to introduce a more complex Third Generation (3G) networks which is based on the Code Division Multiplexed (CDM) technologies with its other flavors, e. g. Wideband Code Division Multiple Access (WCDMA), Asynchronous Transport Module (ATM) in the transport layer for the Universal Mobile Telecommunications Systems (UMTS), (Maye and Morvan, 2006; Nicolas and Pierce-Nenri, 2003).

Following development of the internet, the General Packet Radio Services (GPRS) was introduced to handle packet data services in GSM network. An additional Internet Protocol (IP) network infrastructure was introduced along with new services platforms, e.g. the Multimedia Messaging Services (MMS). Information Technology components such as Network Management System (NMS) and Operations Support Systems (OSS) needs to be enhanced to be able to properly monitor and manage GSM network elements end-to-end (Nicolas and Pierce-Nenri, 2003). Hence, network monitoring tools are sufficiently implemented in network operation and maintenance.

This research work seeks to explore the implementation of the operations and maintenance functionalities called the Operations Support Systems of Airtel Networks and possible areas of improvement. The OSS is the functional entity from where network operators monitor and control the entire Mobile systems.

The complex environment in a GSM/UMTS networks has made it imperative for Service Providers to ensure more resilient network architecture and the use of object oriented software e.g. C++, java and Relational SQL Database (Hughes, 2006) for specific tasks implemented in the OSS with minimal errors expected in the algorithm has also become important. But, network operations are usually bedeviled with all sorts of faults and network errors despite the advancement.

To help mobile service providers meet these new challenges with a better quality of services and to facilitate the smooth integration of multi-technology; the OSS has evolved into a most important element in a typical GSM network (Dereviere and Verbaus, 2003). Hence, the need to ensure that network monitoring tool is provided across all network elements.

The OSS have been designed as an open solution that helps mobile service providers meet the challenges and analyze how network faults could impact negatively on the network performance. There are many different reference models, technologies, system tools to cover the various functions of GSM network management. In terms of the reference models, the most well known model include the International Standards Organization Fault, Configuration, Accounting, Performance and Security (ISO FCAPS)

management systems; ITU Proposed the model called Telecommunications Management Network (TMN). The newer ones proposed by the Tele- management forum is called Telecoms Operations Map (TOM) and enhanced Telecoms Operations Map (e- TOM) (Paessler, 2007; Wendel, 2009).

This Work focuses on FCAPS model which is overlapping with the most popular traditional models deployed by any service provider called Operations, Maintenance and Provisioning (OAM&P).

There are many network management technologies and protocols which addresses some of the network management functions, the most popular being deployed is Transmission Control Protocol Internet Protocol (TCP/IP), Simple Network Management Protocol (SNMP) defined by IETF and Common Management Information Protocol/Service (CMIPs) defined by ISO.

As a prerequisite for ensuring better network operations, the OSS which comprises of the NMC and OAM&P systems is made possible with the various software implementations across all GSM Network Elements (NE). It is important to state here that Network operators deploy equipments from different manufacturers as they are all based on the same open standards, but one major disparity between them is that each has its own specialized software features for managing and monitoring such equipment.

1.2 Thesis Motivation

The OSS has been designed as an open solution that helps mobile service providers meets the challenges of service delivery and the desired Quality of Service. It is also important to realize that customers are willing to pay for new services that meet their needs which are delivered with perfect quality and as per Service Level Agreement (SLA).

Naturally, the mobile service provider will rely on NMS (OSS) systems to provide real-time fault, performance, and configuration management for their network. As new services are introduced by network providers and network expand; the traffic load (and or processor load) will increase, hence, the need to have their network management systems grow to accommodate these new services platform for effective end-to-end network management and event monitoring through the implementation of an effective Software Management System. The emerging services being introduced in Nigeria by Mobile Service Providers (MSP) are not yet being managed and monitored properly.

This research work will investigate the Airtel's network performance in this regard and explore the different techniques of services provisioning and holistic approach to integrated network management systems for a better and more robust network operation.

The desire to have GSM network operations devoid of longer downtime due to network errors; be it hardware or software, and faults detected as fast as possible before they cause potential service disruption in the form of degradation of performance and loss of revenue (increased COPEX) in mobile services provisioning and network operation is the singular most important drive of this work.

Although the field of state-of-art integrated Network Software Management Systems is relatively new in research community, efficient and effective Network and Element Management Systems which forms the heart of a Mobile Network Operations Center for network monitoring on all levels needs thorough consideration.

1.3 Statement of Problem

The real time nature of today's mobile telecommunications networks adds to the difficulty of the fault management systems e.g. a diagnostic system must be able to handle alarm notification flow as soon as they are generated. The maintenance of an accurate model of an integrated mobile network configuration is critical for the fault management system. However, efficient tests including software management needs to be performed on a regular basis to ascertain the true state of Network's Quality of Service (QOS).

The Network Management systems information gathering tools needs to be partially (not wholly) automated and their results consistently interpreted to help the diagnosis and decision process after proper analysis of complex Software fault management data and error logs. Software faults are an integral part of the world of wireless (GSM) technology due to so many reasons: Software patches and code errors i.e. wrong parameterization of software, Interference, program execution errors and Mean Time to Failure (MTTF) including but restricted to Mean Time to Repair. Given the complexity and size of network Software alarms, filtering and correlating the large volumes of data (Error-logs

messages) and choosing the correct tool/technique from the large set of tools available to carry out the Fault trend analysis requires great effort.

The alarm represents the symptoms and as such there are two real world concerns: The sheer volume of alarm events as network software errors are logged and modelling of the causes/effects of fault types. There are no software that simulates the Cause/Effect elements of Network events error-log, Hence, an accurate model based on both Structural and empirical parameters needs to be used to analyse the summary of network error-log messages. Also, using derived error-log message summary of a peculiar data from a live network to validate the Bayesian Inference technique proposition: Posterior x Evidence = Likelihood x Prior, getting posterior probability is always difficult. Thus, resolving the Likelihood and the prior probabilities is far more easier but rarely undertaken for Fault Management task; either as a result of the difficulty in getting data or unavailabilty of database of the previous error-log messages.

1.4 Thesis Outline

The thesis is made up of five chapters. Chapter one is Introduction which comprises of: Preamble, Thesis Motivation, Statement of Problem, and Thesis Outline. Chapter Two is Literature Review and Theoretical Background. Chapter Three consists of Design Methodology and Data collection. Results and discussion formed Chapter Four while Chapter Five covers Conclusions and Suggestions for Further Work.

CHAPTER TWO

LITERATURE REVIEW AND THEORETICAL BACKGROUND

2.1 Literature Review

The wireless communications system used in real commercial services could be traced back to the 1940s when Bell Laboratories of the United State (US) conducted commercial mobile wireless communication systems tests. In the past, communications systems were made of Analog Circuits basically and are made of large-scale integrated circuit; but, computer technologies have paved the way for the rapid development of the commercial applications of mobile communications system as they are now digital (i.e. they can accommodate a good number of services platforms) that was not possible with the analog systems (Shewzen, 2003).

Ever since the cellular theory was put forward in the 1970s, cellular mobile communications have found extensive applications. In addition, as a result of the development of micro electronics/computer technology communications, great progress has been made in mobile communications network management applications.

The Operations and Support Systems have witnessed a more tremendous improvement than any other subsystems in the GSM Network's architecture and Network Elements. This can be readily attributed to the aforementioned development in the areas of integration of computer systems into telecommunications network infrastructure on one hand and on the other hand, giant strides made in the field of software engineering with which comes a new concept of high level programming languages for easy

conceptualization, visualization and abstraction of any complex objects to be managed in modern communications systems.

Thus, the cellular mobile communication system has come through changes from analog to digital and from Frequency Division Multiple Access (FDMA) to Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA), which represents the evolution from the first generation mobile communications system to the third generation (3G) systems.

Quite a number of works have been done and a lot more on-going researches aim at standardizing and integrating the implementation of OSS for Mobile Networks (GSM). Distaso (1980), explored many of the problems plaguing Network Operation and proposed how Software (S/W) management practices may be employed in dealing with the problems of automated engineering tools. In the work, he presented a means of ensuring communications between the various network elements and for maintaining a high degree of visibility and accessibility through properly designed software program.

Wallstrom (2007) conducted a practical study at Helsink University of technology to address the need for an Automated Mobile Radio Network Performance and Fault Management System in a typical NMS (OSS). The process follows the root-cause analysis methodology by getting top level performance management data and Network error logs, and alarms trapped for Fault Management Analysis. After Investigation (Performance Management) and then Analysis (Fault Management) phase, The Decision

phase which maps to software management and configuration management were considered and each phases of the process has deliverables that are utilized in the latter phases.

In addition, a method to locate and correct software errors within a protocol stack for wireless devices (Mathew, 2004) was invented at BroadCom Corporations. A set of software tools that converts case logs from wireless Network Elements to simulation scripts which may be used to test protocol stacks implemented in GSM networks were considered.

It was observed in a white paper (David, 2007) that as with any other network services, guaranteed service levels as per service level agreement and performance management reporting are the critical factors in optimizing the performance of the infrastructure. The white paper discussed some challenges of performance management and Fault Management solutions. In order to do this effectively; they need comprehensive and flexible system that reports on the key performance Indicators (KPI) as it affects alarm generation reporting and vice versa.

Further work was done on the OSS/BSS systems for a Next Generation OSS. In the white paper, the Generic enterprise architecture for integrating the OSS/BSS system for a mobile telecoms provider was proposed (Hughes, 2006). The proposed architecture is based on Services Oriented Architecture (SOA), which does not offer end-to-end network management tool that is essential to structure and reduce integration complexity.

Recently, similar works was done by Nokia Siemens Network in an attempt to provide flexible and implementable common OSS architecture based on existing industry standards and promoting the use of re-usable OSS software component (Paessler, 2007). It was also noted that the traditional approach to building propriety EMS/OSS architecture is no longer sustainable. Consequently, the problem of adapting and integrating Network Elements and OSS would be solved in a multi vendor environment.

In a recent work, mobile agent technology was used as a potential tool for realizing distributed network fault management. The actual focus was on the application of intelligent software agent using probabilities model as inference engine for fault management. It was Bara and Mykoniatis (1998) who designed this integrated distributed belief networks fault management system. Similar work was done by John and Clement (1980) who approached software reliability modeling of network faults error-log messages from an empirical viewpoint using both conceptual and predictive approach which produces a more superior Software model.

The various approaches to the works considered here so far are quite interesting. A critical review of the literatures shows that they were either silent on a particular management functions when considering the automated mobile communication management structures or they fail to address the integrated mobile Network management implemented at the OSS (NMC) of Network Service Providers.

The main thrust of this work is therefore to consider the implementation of an integrated network management system that takes into consideration; the parameters that affects Network overall performance with reference to network Alarm/Event parameters.

2.2 International Telecommunications Union FCAPS & OSS Framework

The Telecommunications Management Network (TMN) model was introduced by ITU as a reference model for the Operations Support Systems (OSS) of telecommunication service providers. The TMN concept is an architectural framework for the interconnection of different types of OSS components within the Network Elements (NE). TMN also describes the standardized interfaces and protocol used for the exchange of information between OSS components and NE, and the total functionality needed for network management (Nicholas and Pierce-Nenri, 2003). The TMN model comprises of the following four layers:

- Business Management Layer: Performs functions related to business aspects, analyze trends and quality issues; for example, to provide a basis for billing and other financial reports.
- Service Management Layer: Performs functions for the handling of services in the network definitions; administration and charging of service.
- Network Management Layer: Performs functions for distribution of network resources; configuration, control and supervision of the network.
- Element Management Layer: Contains function for the handling of individual network elements. This includes: alarm management; handling of information backup; logging and maintenance of hardware.

At each layer in the TMN model, five functional areas called FCAPS are defined.

Each TMN layer needs to perform some or all FCAPs functions in certain ways as illustrated in Fig 2.1.

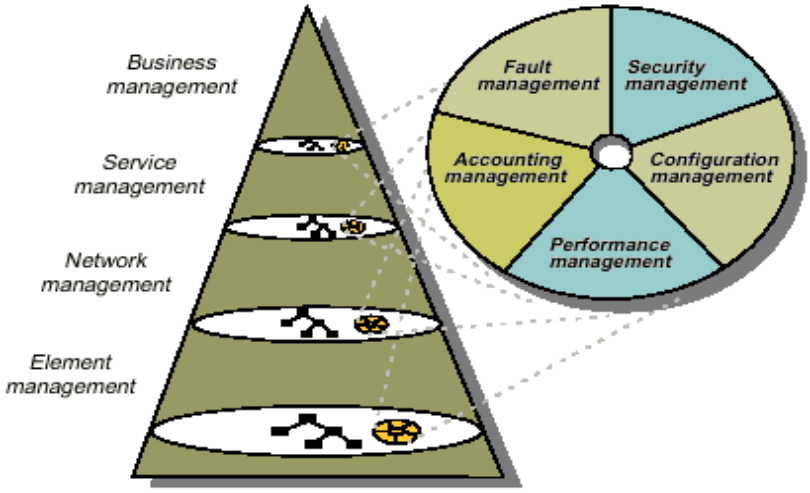


Fig. 2.1 Mapping between TMN reference model and the FCAPS.

(Source: ITU Recommendation M. 3000 at www.itu.org)

The Operations and Support Systems which comprises of the Network-wide Management Systems (NMS) and the Operations and Maintenance Systems (OAMs) is connected to all Network Elements from Mobile Switching Center to the Base Station subsystem and is itself a major subsystem in a Mobile service providers infrastructure (Fig. 2.2). The equipments have specialized interfaces from each network elements to the NMC, and the OSS centralized database provides the means to supervise network elements via an SNMP interface. OSS Interface framework (Q3 Interface) forwards alarms and network element events to the NMC.

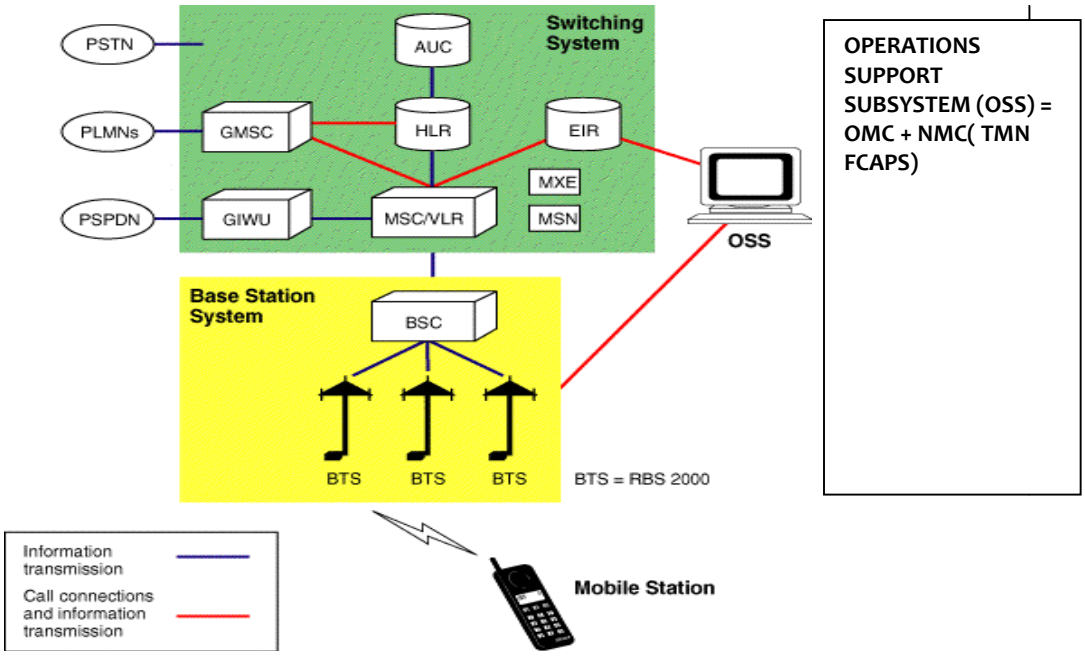


Fig. 2.2 GSM Network Architecture and OSS

The purpose of the OSS is to offer the Service provider cost-effective support for centralized, regional and local operational and maintenance activities that are required for a GSM network. An important function of OSS is to provide a network and its increasing business services including Voice, Data, and Multimedia effective network operations at the desired quality of service and as per service level agreement.

This thesis focuses on the current and near future states of OSS technology and its developmental stages to support new and emerging services and technologies for the future. It is also intended to cover only the Network Management and Element Management layers of the Telecommunications Management Network (TMN) model with special emphasis on software fault management systems which is part of configuration management functionality of the ITU-FCAPS Model.

2.2.1 Fault Management

Faults are an integral part of the world of wireless GSM technology due to so many reasons: e.g. frequent disconnection in the air interface, narrow bandwidth, lack of resources and high mobility (John and Clement, 1980). Hence the necessity of providing better fault tolerant mechanism for ensuring reliable working of a GSM network cannot be overemphasized.

Fault management systems is a set of functions that detect, isolate and correct malfunctions in communication network, hence, the goal of fault management is to detect, log, notify users of errors and (to the extent possible) automatically fix network problems to keep the network running effectively, faults (Software or Hardware) can cause prolonged downtime or unacceptable network degradation. Fault management is perhaps the most widely implemented of the ISO Network Management Elements (Masud, 2006).

Also, fault management system helps to detect faulty software and fix them automatically or until technical personnel clears such software faults as alarms. Fault management includes all those procedures necessary to handle software alarms; filters and correct faults, and then respond intelligently to customer complaints.

Most Networks locate these errors in software as they happen using mobile agents i.e. application SW components contained in the device (NE) that are to be managed. This initiates series of steps to clear and repair the fault, or minimize the impact either by

software or hardware means (Karmouch and Pharm, 1998). A good fault management system should be able to collect relevant fault management data i.e. NE logs, configuration Data and alarms for troubleshooting.

2.2.2 Software Management

Nowadays, GSM world is a new software paradigm that is of prime interest in the IT research community. As a prerequisite for ensuring a better network operation, the Operations Support Systems which comprises of the Network – wide management systems and the operations, and maintenance system is made possible with the various software platform implemented across all Network Elements from Base Station to the Mobile Switching Center (MSC).

The complex environment in a GSM/UMTS networks has made it imperative to ensure a more resilient network, architecture and the use of object oriented software for specific tasks e.g. (C++ and Linux UNIX implemented in the NMS (OSS) with little or no errors in the original algorithm. To help mobile services providers meet these new challenges with a better Quality of Service (QOS) and to facilitate the smooth integration of multivendor equipments, NMS should provide mediation amongst all NEs including Network Management Center's (NMC's) stable standard interfaces, service provisioning activities must be automated through ensuring that the software errors are kept minimal. It is not possible to have an error – free network operation though.

All Network Management Systems are based on a consistent set of common software platforms across the various sub-network managers. This platform provides the glue needed to build homogenous management system across all sub-networks.

This software architecture is modular enabling new element managers to be added easily without affecting other functions. The application framework is based on client server architecture. The server part of each application can be distributed on several physical servers, providing scalability required in meeting the growing demand while the client part of the application enables operator workplaces to be distributed either locally or at remote locations (Daniel, 2005; John and Clement, 1980).

Software management covers software request management, installation, customer feedback and software fault management i.e. detection of software faults and finding resolutions to the problems, this duty is close to/and overlapping with Fault Management (FM) functionality. Software Management includes a wide range of task and can be viewed to certain extent, as part of configuration management. Software management includes the management of existing software versions in operation, the installation of new hardware with the latest software versions and control resolution of software problems, this is a major task in the software management process which includes the problem analysis over a certain period of time and across regional network operation centers while maintaining the consistency of the technical operational database (John and Clement, 1980).

2.3 Fault Diagnosis System Based on Bayesian Networks

Bayesian Decision Theory is one method used to solve *Pattern Recognition* problems; when those problems are posed in a particular way. Bayesian decision theory plays a role when there is some *prior* information about the things we are trying to classify. In NMS, Faults occurring in network operations are always seen as a random distribution and hence modeled as such. This probability distribution plays an important role in formalizing the decision rules.

In this work, we hope to explore the importance of the ‘’Prior’’ information in the pattern recognition problem (alarm correlation) and will provide some exact formulas for decision rules that use probability distribution. To evaluate the probability of a hypothesis, the Bayesian probabilistic theory specifies some Priori Probability which is then updated (validated) in the light of new relevant data. The Bayesian Probability interprets the concept of Probability as a measure of a state of knowledge in contrast to interpreting it as a frequency or a physical property of a system (Jaynes, 2003).

Broadly speaking, there are two views on Bayesian Probability that interprets the state of knowledge concept in different ways. According to the objectivistic view, the rules of Bayesian Statistics can be justified by requirements of Rationality and Consistency both interpreted as an extension of Logic (Richard, 2001).

2.3.1 Bayes' Theorem

Bayesian theory states that: "given some data and some hypothesis, the posterior probability that the hypothesis is true is proportional to the likelihood multiplied by the prior probability''. The likelihood brings in the effect of the data, while the prior specifies the belief in the hypothesis before the data was observed.

In general, Bayesian methods are characterized by the following concepts:

1. The use of Hierarchical Models and the marginalization over the values of nuisance parameters (approximation by Markov Chain Monte Carlo) like Frequency of occurrence
2. The sequential use of Baye's formulas: when more data becomes available after calculating the posterior distribution, the posterior becomes the next prior.
3. In frequentist Statistics, a hypothesis is a proposition which must be either ''true'' or ''false'', so that the frequentist probability is either ''1'' or ''0''.

More formally, Bayesian Inference uses Baye's formula (2.1) for conditional probability;

$$(\quad /) = [\quad (\quad /)P(\quad)]/ [P(\quad)] \qquad (2.1)$$

Where: H is a hypothesis and D is data, P (H) is the prior probability of H i.e. Probability that H is correct before data was seen; P (D/H) is the conditional probability (Likelihood) of seeing the data D given that H is true; P (D) is the marginal probability of the Data D; P (H/D) is the posterior probability that the hypothesis is true, given the data and the previous state of belief about the *hypothesis*; and P (D) is the prior probability of witnessing the data D under all possible hypothesis as the Evidence.

Again given any exhaustive set of mutually exclusive hypothesis H_i, we have:

$$( ) = \sum (,) = \sum (/) ( ) \quad (2.2)$$

We can consider *i* here to index all ''classes of faults'' in the network, is the hypothesis that the faults will always occur. (,) is then the probability that the fault occur with a set of symptoms; since the set of alternative faults was assumed to be mutually exclusive and exhaustive, this is a case of Total Probability. ( ) is the normalizing constant, which in many cases needs to be evaluated (Aldrich and Stephen, 2008; Lucien, 1986).

2.3.2 Bayesian Networks

Telecommunications networks error-logs are characterized by their structure and behavior, knowledge of these are modeled using rules that are based on known faults. These model-based systems comprises of well structured fault scenarios which can graduate from being reactive to proactive and even go on to becoming predictive in nature for fault diagnosis i.e. a form of artificial intelligence systems.

The Bayesian Model paradigm more than meets the requirements for this model-based system. Although the development of the model-based reasoning has to be completed before knowledge-based reasoning artificial intelligence systems can be developed.

Baye's Theorem stated mathematically thus:

$$- = - * ( ) / ( ) \quad (2.3)$$

$$( ) = - * ( ) / - \Xi \sum (,) \quad (2.4)$$

Where: P (D) is the marginal probability of witnessing the data under all possible hypothesis; $- * ( ) / -$ is the joint probability that the faults occur with sets of symptoms. Hence, if we assume that the sets of alternative faults are mutually exclusive, then,$\sum$ (,) defines the Bayesian Network model. P (D) is the normalizing constant which will be evaluated.

The Bayesian network is a pair (D, H) that allows efficient representation of a joint probability distribution over a set of random variables U= $\{X_1,\ldots\ldots\ldots\ldots X_n\}$, D is a Directed Acyclic Graph (DAG) whose vertices corresponds to the random variables X and whose edges represents direct dependencies between the variables (depicting the Causes & Symptoms).

The second component H is a set of conditional probability functions; one for each variable;

$$= \{ (/),\ldots, (/)\} \qquad (2.5)$$

Where; is the parent set of X_i in U, the set H defines a unique joint probability distribution over U given by:

$$( ) = \frac{\Pi \quad ( )}{} \qquad (2.6)$$

In this work, the DAG will be used to encode the causal relationships between particular variables represented as nodes. Nodes are connected by causal links represented by arrows which points from parent nodes (causes) to the child nodes (effects or symptoms) and vice versa. Each node in the resulting network has associated with it a conditional probability that quantifies the effects that the parents have on the nodes (Baras and Mykoniatis, 1998; Lauritzen and Spiegelhalter, 1998). Taking the graph as a whole, the

conditional probabilities and the structure can be used to determine the marginal probabilities or likelihood of each node holding one of its states.

Bayesian Networks are practically applied to model causal inference systems where the cause/ symptoms of faults are modeled as the nodes of a BN, while the edges represent the cause-effect relationships between these entities. The qualitative part of a BN is encoded in the structure of the diagraph and the conditional probability distribution for the nodes encodes the qualitative portion (Cooper, 1990).

Bayesian Networks based on probability theory uses the Causal Inference and Diagnostic Inference Techniques. The causal inferences reason as a result of variables (fault types) from the given causes and the diagnostic inference reasons as a result of symptoms only (Sahoo and Oliver, 2002; Lauritzen and Spiegelhalter, 1998).

2.4 Software Reliability Concept

Reliability is the characteristic of an item expressed as the probability that it will perform a required function under stated condition for a given period of time. The Mean Time between Failure (MTBF) is an extremely important characteristic in reliability predictions. It can be computed as the mean value of the length of time which elapses between failures. In terms of network fault analysis, MTBF is not as relevant as Mean Time to Repair (MTTR). A growing proportion of the Mobile communications network management systems operate in real time and the operational cost/impact of software malfunctions are enormous as hardware faults are generally less complex than software faults (John and Clement, 1980). With the advent of microprocessors; hardware faults

have been kept minimal with software running in the background. A failure is an unacceptable departure of program or piece of equipment operation from the specified requirements; hence, a fault in the software causes equipment failure while the term error is used to indicate the network action that results in a fault (Glossoler, 1978).

The Mobile service provider (MSP) may wish to establish several classes of failures of differing severities and define reliability requirements for each class. The foregoing definition of Software reliability is an operational one and it has been adopted because it offers the greatest management utility to MSPs. In our analysis, we will think more in terms of the number of faults, i.e. errors occurring during network operations and the effect of software errors that affects both logical and physical network parameters in form of alarms. Reliability (denoted as R (t)) represents the probability that failure will not occur in time t, let the expression in (2.7) represent the probability that there will be a failure of any kind: i.e. let

$$F(t) = 1 - R(t) \tag{2.7}$$

represents the probability that failure will occur in time t, and then the Hazard rate Z (t) represents an instantaneous failure rate with respect to time or the failure rate given that a system or component has survived until now. Thus,

$$( ) = \frac{( )}{( )} \tag{2.8}$$

( )is the failure rate w.r.t. time t. It is readily shown that:

$$( ) = \int ( ) \tag{2.9}$$

The mean time to failure T is the expected value of the failure interval; it can be related to reliability as follows:

$$= \int \quad ( ) \tag{2.10}$$

If the failure rate is not constant, then the expression in (2.10) becomes:

$$( ) = \tag{2.11}$$

For small t, ( )=1- , (is the hazard rate). Hence, T=1/ for repairable faults as the MTTR. The failure rate or hazard rate could also be looked at as the sum of random processes Ø ,where each Ø is associated with a particular fault

$$= \sum \quad Ø \tag{2.12}$$

Where N represents the total number of inherent faults in the system and n is the Number of faults detected. The distribution of each of the Ø can be found from Bayes' theorem. Availability may be computed for software as it is for hardware, availability is the expected fraction of time during which a system will operate satisfactorily. If we let the time interval over which the measurement is made approach infinity, then the availability is given by:

$$= \frac{}{} \tag{2.13}$$

Where A is the availability, T is the MTTF and F is the MTTR which is ordinarily determined as the average time required for restoring networks to normal operation (Oroge, 1991).

2.5 Software Alarm Filtering and Correlation Techniques

Research studies in automation of diagnosis in the Radio Access Networks (RAN) OAM & P activities of Mobile Service providers' network have been focused on alarm correlation (Frolic, et al, 1997). The aim of the automatic diagnosis system is to identify the causes of a problem based on the values of some symptoms. In current cellular networks, most systems are semi-intelligent and generate alarm messages when errors occur with very low level of abstraction and this normally leads to a high number of alarms for any single cause. Alarm correlation consists in the conceptual interpretation of multiple alarms so that new meanings are assigned to the original alarm (Wietgrafe, 2002; Yang, 1997).

In a large system, the number of alarm records is large; to diagnose a network problem by manually examining alarm records is very difficult but a necessary requirement for efficient and conclusive diagnosis. A summary of information about the alarms will be helpful to the network administrator. In addition to summarizing alarms, the outage analysis system will perform series of actions to determine whether the detected outage constitutes a false outage or true alarm (Hawkins et al, 2009). Filtering and correlation are two important aspects to be considered to make the separation of the principal faults from its side effects easier. Indeed, the physical and air interconnections of network components and the logical dependencies between the distributed software modules lead to multiple manifestations of the same fault.

Quantitative and qualitative models can be used to predict which components are likely to contain the highest concentration of faults based on adequate software metrics and log

of faults found by testers and clients of software systems. To develop such systems, a complete understanding of Network Management principles is required. This is valid for mobile radio networks where an efficient fault management system should reduce the outage time of radio and other communicating resources is achieved by means of an automated analysis of the alarms generated and by an automated diagnostic process. It is based on results of the alarm filtering correlation that a fault diagnosis is made; this can vary from simple message filtering and redundant alarm suppression to a more sophisticated alarm compression and generalization techniques (Boix and Svedberg, 2008; Carls et al., 1997).

2.5.1 Rule-Based (Model-Based) Systems

Many factors come into play in the process of event correlation. The two most important aspects of event correlation system are: the speed with which correlation occurs and the accuracy of the data returned by correlation process. A system must have an accurate and appropriate combination of these characteristics in order to be considered effective.

A somewhat traditional approach to event correlation is that of Rule-based analysis; in this approach, sets of rules are matched to events (cases) when they come in. Rule-processing engine analyzes data (correlate and match) until it reaches the final state, and then reports the diagnosis (Liu and Yang., 1999). There are different techniques for processing the modeled information. For Knowledge Based Systems (KBS), the processing is handled by an inference engine using reasoning techniques such as model-based and case-based reasoning. Telecommunications network are characterized by their structure and behavior, knowledge of these characteristics are modeled using sets of rules

that are based on known faults. A detected symptom is matched against these rules in order to find the root cause (Boutabi and Dovik et al., 2000, p. 20).

2.5.2 Code Book Systems

The Code Book approach is somewhat similar to the model-based approach, but rather than treating events separately, they are grouped into an alarm vector which represents all of the events. This alarm vector is then matched to problem signatures in a so called codebook; in these systems, no two alarms have the same signature. In order to optimize performance, a system should use small sets of symptoms while still providing the best guess of the cause. This can be done in the creation of the codebook by forcing a minimum Hamming Distance, a measure of differing symptoms between different causes and by reducing otherwise indistinguishable cases into one which encompasses all of them (Binay and masum, 1999). The system is faster (though it still needs expert knowledge to populate the codebook) because there is less comparison for each event and empirical data has proven difficult to come by from the Mobile Service Providers.

2.5.3 Artificial Intelligence Systems

There are many different types of Artificial Intelligence (AI) Systems and Event Correlation techniques have been proposed which utilize various combinations of them; this includes both Bayesian Belief Networks and Intelligent Management Information Base (I-MIB) expert systems. I-MIB is the conceptual information store for all management aspects of TMN. Model-based reasoning accounts for the Intelligence in the

I-MIB by integrating reasoning capabilities with the MIB (Herman et al., 1997; John and Williams, 1996).

Information required for the management of the network resources also includes a Knowledge Base, having knowledge such as the behavior of the Managed resources in a given fault scenario or a propagation path of a known fault. I-MIB is encapsulated in an agent who not only performs the classical and simplistic role of a standard agent that searches for management information on Managed Objects (MOs) (i.e. invoking control primitives on MOs); it is also in charge of maintaining knowledge models and management information of network resources (Herman et al., 1997).

I-MIB is a common core for network OAM & P and may be distributed logically and physically to suit the distributed nature of Mobile Network architecture. This technique is suitable for applications which can be reduced to a small set of already known cases; this means that the development of the model- based reasoning has to be completed in order for the knowledge-based reasoning capability of AI (I-MIB) to be available. This further helps to lay the foundation for the integrated mobile network management system based on analysis of known faults after carrying out performance tests. Bayesian modeling (Bayesian Belief Networks for identifying faults), Fuzzy Causal probabilistic Network and Neuro-Fuzzy Inference machines are the main tools used to realize the AI Systems as regards automatic diagnosis in mobile communications networks (Yang, 1997).

2.6 Integrated Diagnostic Techniques Based on Neuro-Fuzzy Inference AI Systems

A single strategy for diagnosis does not seem to be suitable especially for complex problems in mobile network's fault management tasks. An integrated diagnostic technique based on AI approach is superior because complex systems inevitably require real world hybrid solution. A combination of fault-based reasoning, Model- based reasoning and quantitative models (i.e. simulations and numerical models) together with qualitative models (i.e. structural behavior and functional black box models) helps to establish the observed behavior of the system and should be able to predict the symptoms based on previous fault cause.

Expert systems are computer programs employing programming techniques found in the field of Artificial Intelligence known as Knowledge – Based Systems. These computer programs are designed to apply formal representations of domain knowledge or expertise to solve problems using symbolic descriptions in the form of ''IF THEN ELSE'' rules; for example:

Function foo (X1 as variant, X2 as variant)

On Error Goto Handle_Error

If aClass is nothing Then

Set aClass = New mycomponent

End If ' (call some method on aClass)

Exit Funcion

Handle_Error:

Foo = Error. Description

End Function

The definitional and empirical relationships in a domain and the procedures for manipulating them compared to conventional programming methods is different, the emphasis in developing expert systems is placed on processing information at the knowledge level rather than at data-level because of its Inferential capacity. This allows an information processing agent (the inference engine) to navigate from a set of observation to the identification of problem symptoms; from a set of symptoms to a diagnosis and to a recovery plan of action. These procedures are generated dynamically as the inference engine of a knowledge based system matched the current inputs to relevant Elements in the network and helps to re-assess the state of a situation during each cycle of a reasoning mechanism (Riverrol and Sanctis, 2005).

Neural networks are sometime useful for alarm correlation taking into account the dynamic nature of growing cellular mobile networks, such an Artificial Intelligence system needs to be efficiently adapted to different topologies of network structures as well as to new and additional Network Elements. If an Alarm Vector belonging to an initial Cause is known, the neural network can be trained to transform the original alarm vector into the initial cause.

If the initial configuration of the network is modified, the input and output layer of the neural network is adjusted and the new alarms with the initial cause pattern just have to be trained again. Fig. 2.3 shows the principle of mapping the alarms from different network elements to the neural network. An alarm is represented by a neuron in the output layer, during training; the weights of the connections are trained and adapted, and

the state of no alarm is noted as -1 not 0 with the active alarm state presented as 1 at the corresponding input neuron (Towel and Shavlik, 1994).

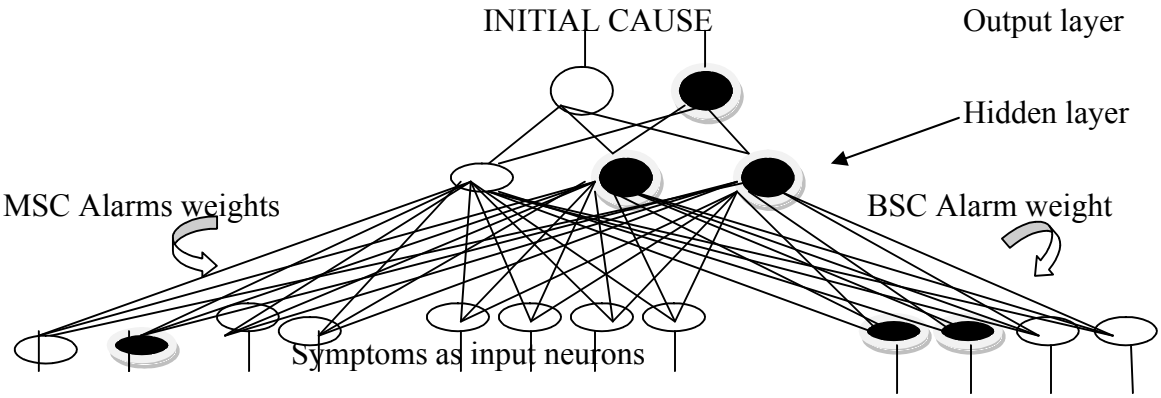


Fig. 2.3 Alarm Mappings to Neural Networks.

CHAPTER THREE

DESIGN METHODOLOGY AND DATA COLLECTION

3.1 Introduction

Traditionally, Log files were not only intended to be read by humans in order to support fault diagnosis but also to be used for root- cause analysis after a system has failed. The raw data so obtained are not suited to trend analysis for proper fault diagnosis, hence, the need to first filter the raw data before correlating the parameters for modeling. After Filtering and Correlation of the error- log message to obtain the summary of alarms for both the Base Station Controllers (BSC) and Mobile Switching Centers (MSC) using some advance filtering and sorting; the compressed alarm is now used for the Fault trend Analysis and Bayesian modelling of derived parameters

3.2 Methodology

- *Network Elements (NE) Software alarms and error logs i.e. overall network error- log message from NEs like, BSC and MSC of Airtel Network was collected for a period of Three (3) Months.*
- *A method called 'Tupling' will be used to filter the raw and voluminous error log messages at both the BSC and MSC.*
- *Fault Trend Analysis of Alarm Summaries will be used to classify (correlate) Network faults using criteria like: Priority, nature and hierarchy of faults that are gathered.*
- *Statistical tools (Area Chart) will be used for the Fault Trend Analysis of the derived summary of alarms.*
- *Bayesian modelling will be used to model error- log message summaries.*

- *Formulate our knowledge of the situation probabilistically by defining the model that expresses quantitative aspects of the known parameters using the following expressions from Bayesian Theorem to specify the marginal probabilities and the conditional probabilities of known fault types given the cause(s) respectively,*

$$(\ ) = \prod \quad (\vdash),$$

$P\ (S_i=S_{i,j}\ / C=C_k)$

where, is the parent set of X_i in U, the set H defines a unique joint probability distribution over U, X_i ($S_{i,j}$) is the random variable i.e. the symptoms, and C_k is the prior probability of the cause.

- *A standard Conditional Probability Table (CPT) of fault type's conditional probability distribution will be computed by dividing the appropriate marginal.*

- *Matlab simulation of the proposed Intelligent Management Information Base (I-MIB) system and its interaction with analyst systems (Relational Database) using the Matlab Database Toolkits GUI tool.*

3.3 Data Collection

The data used in this work was obtained from AirTel Networks Network Management Center, Lagos. Error log files of network elements like: MSC and BSS (BSC) consisting of error log-Messages was collected for a period of three (3) Months (January, 2010 to March, 2010); (See Appendix 1 A and B). The Dataset consists of error-log messages with a total of 10,000 logs of fault each from the MSCs and the BSCs. In analyzing the

huge data set obtained; such failures that are related to power and those that occur due to climatic changes were truncated (filtered) as redundant alarms to be stored in another log file, because we are only interested in software alarms that have direct impact on network performance. The remaining software alarms were filtered for correlation analysis and modeling.

3.4 Presentation of Derived Parameters

Error-log messages often contain events that are related to a specific fault due to parallelism in the system; these events are interleaved with unrelated events. These can be seen as noise in the dataset which needs to be filtered before correlation of the faults.

Repetitive log records occurring more or less at the same time are frequently multiple reports of the same fault. A method called Tupling (Daniel and Tsao, 1983) which basically refers to grouping of error events that occur within some time interval or that refers to the same location in a managed communications network is introduced as a correlation measure for this purpose. Alarm correlation consists of detecting commonalties between alarms; determining the principal alarms and redundant alarms (with the aim to discarding their side effects), then the correlation process now graduates from simple message filtering and redundant alarm suppression to more sophisticated alarm compression and generalization (Jacobson and Weisman, 1993). Applying this algorithm to the error logs resulted in an immense reduction of the number of alarm reports.

Meanwhile, the following expressions were used in turn to filter and correlate the raw data in MS Excel as advanced sorting and filtering techniques:

=COUNTIF (range, ‘‘error log name’’) (3.1)

This was used to count the total number of occurrences of each fault types over the total sample size of 10, 000 separate error log-messages.

And;

=IF(E8=30,(MID(F8,1,2)*24+MID(F8,9,2)+MID(F8,18,2)/60),IF(E8=29,(MID(F8,1,1)*24+MID(F8,8,2)+MID(F8,17,2)/60),IF(E8=28,(MID(F8,1,1)*24+MID(F8,8,2)+MID(F8,16,2)/60),IF(E8=27,(MID(F8,1,1)*24+MID(F8,8,1)+MID(F8,16,2)/60),IF(E8=26,(MID(F8,1,1)*24+MID(F8,8,1)+MID(F8,16,1)/60),"nil"))))) (3.2)

Which is used for time converting the average duration over the total number of occurrences of each error log-messages; the compressed (correlated) Alarm summaries for the MSCs and the BSCs are presented in appendix 2 (A and B).

Nevertheless, as is always the case for many grouping algorithm; it may assign the same ID to two errors that are not caused by a single symptom and error messages might be combined that refer to several unrelated faults commonly referred to as collision. In this work, different error IDs were assigned to the active alarms from the correlated log files.

CHAPTER FOUR

RESULTS AND ANALYSIS

4.1 Introduction

The twin parameters of "Frequency of Occurrence" and "Mean Time to Repair (duration)" of faults have serious effects on network performance. Stored error-log messages from a life network, after filtering and corelation could result in a well structured fault model. The derived summary of error- log messages obtained was further classified for fault trend analysis and simple Bayesian modeling of the software alarm summary is presented.

MATLAB Simulation of the relational database for error –log messages which help to provide a database of previous faults for the purpose of analysis is also realized. Results are presented graphically so that Fault Trend Analysis and Fault Trees of error –log messages showing variations/behaviour of one measured parameter against another is obtained and inferences used to draw logical conclusions.

4.2 Fault Trend Analysis of Network Elements Error-Log Message Summary

Faults may be classified on the basis of priority, timing properties and nature of the sources of faults. Priority of faults includes the following subclasses: Higher Level priority faults with complete impact and major disturbances on the systems; higher level priority with no impact on call processing but severely affecting specific services or function; lower level priority with external low impact. Although, Fault –based reasoning (FBR) technique is not adequate for detecting novel faults and cannot be updated; it is

still preferred by Network Operators for fault management analysis of all software alarms that are collected from the centralized network management systems.

The other fault management techniques like the Model-based Reasoning (MBR) and Case based reasoning are well structured Fault-based Reasoning (FBR). However, MBR is applicable only where a sufficiently good model can be built from FBR. MBR can detect novel faults while FBR is used to diagnose common faults.

Hence, a fault description model we have combine all these models, thus a problem may have a high priority, a permanent fault, has a software nature and be located at a given Network Element. A basic classification based on the priority was used to analyze the error- logs pattern after filtering of the raw data for correlation.

4.2.1 Fault Trend Analysis of Base Station Subsystems (BSS) Error-Log Message Summary

Trend analysis of the BSC fault summary (Appendix 2A) has shown from careful observation of "Frequency of Occurrence" and their corresponding "Duration" that: they occur more frequently and the higher the "Frequency of Occurrence" the lower the "Duration" (MTTR) and vice versa (Fig. 4.1). Consequently, faults that are of high priority have two parameters that have major impact on network performance, i.e. the "Frequency of Occurrence" and the "Mean Time to Repairr" such faults to restore the network to its normal operation. When the error-log summary is further classified based on priority; the same behavior was noticed.

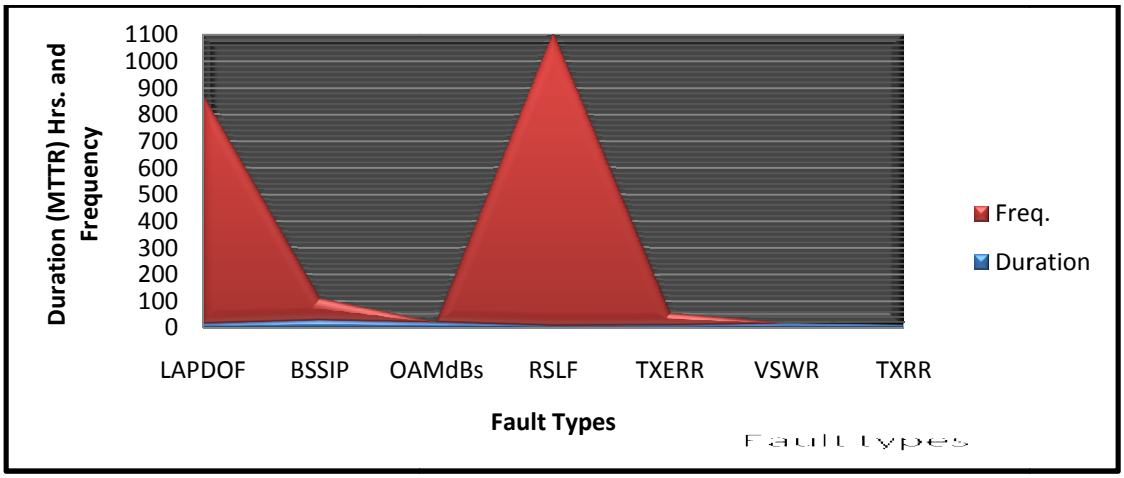
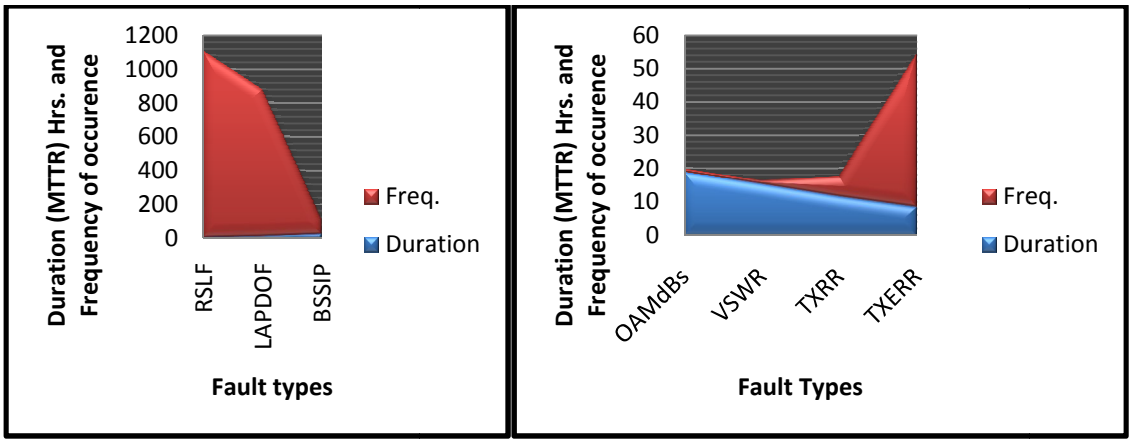


Fig. 4.1 Area Chart Comparing Frequency of Occurrence and Duration for BSS Alarm Summary

The classification of BSS alarms based on Priority is further divided into Subclasses: High Level Priority Faults with Complete Impact on the Network, which comprises of 'BSS Internal Problems', 'RSL Link failed' and 'LAPD_OML Failure'; High Level Priority Faults with no Impact on Call Processing but Severely Affecting Specific Services, which comprises of 'Transmission network error',' VSWR faults' and 'OAM Database not found', the same impact was noticed (Fig. 4.2).



(a) *(b)*

Fig 4.2 Area Chart Comparing Frequency of Occurrence and Duration for BSS Alarm Summary plots comparing BSC High level priority faults: a) with serious impact on network performance and (b) with little or no impact on network performance.

4.2.2 Fault Trend Analysis of Mobile Switching Center (MSC) Error-Log Message

Summary

Table 4.1 MSC classified High priority faults
With major disturbances on the network

FAULT TYPES (SYMPTOMS)	Frequency	Duration	CODES
High Processor Load and Call limiting	2813	7.06	HPLCL
100% C7 link failure	900	12.1	100%C7LF
CP FAULT	137	17.3	CPF
RP FAULT	247	15.96	RPF
CP- AP COMMUNICATION FAULT	54	24.42	CP-APF
GROUP SWITCH FAULT	63	26.14	GPSWF
SOFTWARE ERROR	11	34.12	SWERR
100% devices blocked	41	35.07	100%DB
Not processing calls	12	4.16	NTPRC
NMC is unable to monitor	107	5.5	NTPRC
CP State not Normal	8	62.33	CPSNTN

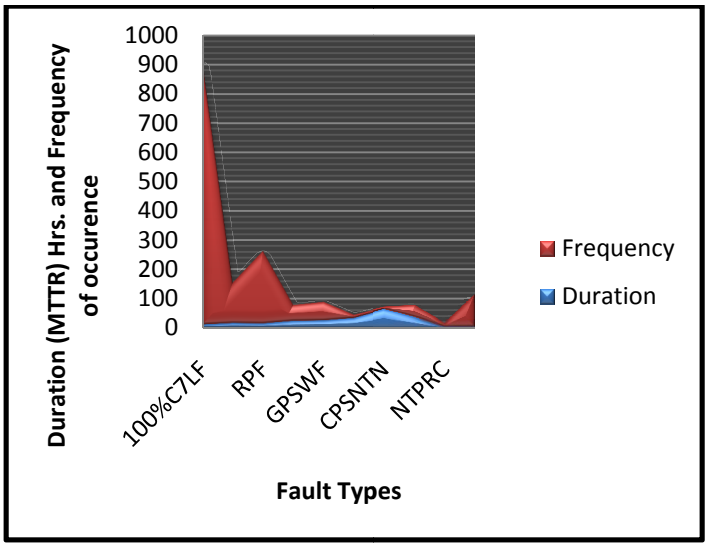


Fig 4.3 Area chart showing the relationship between frequency and MTTR of MSC High priority faults with major disturbances on network performance.

Table 4.2 showing MSC classified High priority faults
With little or no disturbances on the network

FAULT TYPES (SYMPTOMS)	Frequency	Duration	CODES
High Processor Load and Call limiting	2813	7.06	HPLCL
High processor load	106	3.69	HPL
Cannot monitor node	282		CMN
Call limiting	78	2.1	CL
50% C7 link Interfailing	36	6	50%C7LI
CCITT7 LINK FAILURE	222	6.28	CCLF
C7 Link interfailling.	15	1.24	C7LI
Charging destination fault	19	10.67	CDF
OMC not Responding	209	1.82	OMCNTR

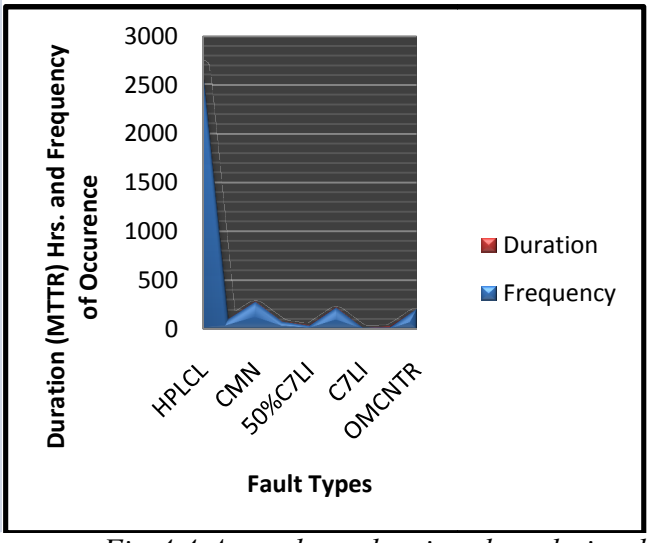


Fig 4.4 Area chart showing the relationship between frequency and MTTR of MSC High priority faults with little or no impact on network performance.

The summary of MSC Alarms shown in Appendix 2 (B) can be classified based on the criterion of priority. MSC faults are very critical to network performance and smooth operation of the entire mobile network due to the nature of the switching equipment and the large volume of software modules implemented for various network operation. The MSC also interconnect all other network elements and the Network Management Systems. MSC Fault Summary was also classified into: High level priority Faults with complete impact and major disturbance on the system (Table 4.1) and High level priority faults with no impact on call processing but severely affecting specific services (Table 4.2)

4.2.2.1 INTERPRETATION OF RESULTS FOR MSC

MSC Fault Summary was also classified into: ‘’High Level Priority Faults with Complete Impact and Major Disturbance on the System” (Table 4.1) and “High Level Priority Faults with no Impact on Call Processing but Severely Affecting Specific Services (Table 4. 2). The same impact the twin parameters of “Duration (MTTR)” and “Frequency of Occurrence have on BSS is applicable to MSC. High level priority faults with major impact on call processing, with few exceptions though. As shown in Fig 4.3; the last two fault types: ‘’NTPRC’’ and ‘’NUTMON’’ occurs 12 and 107 times respectively while their respective duration is 4.16 and 5.5 Hrs. This is a slight deviation from the usual trend that when the number of occurrence increases; the duration decreases this is attributed to the critical nature of these fault types: If the Network cannot process calls and NMC is unable to monitor faults, then the network is being crippled with serious service disruption. Hence, very low MTTR values. For example, 100%C7LF which

occurs 900 times in three months with a low duration of 12.1hrs compared to software error (SWERR) which occur just 11 times but the MTTR is about 34.12hrs. But for those faults that have little or no impact on signal processing; serious deviation from the observed behavior was noticed, here, on the average the MTTR for all fault types in this category is 5 hours irrespective of the frequency of occurrence of such fault types.

These fault types are considered to be of high priority base on two criterions, firstly, they occur more frequently than other fault types and secondly, they are associated with a relatively short MTTR i. e. the duration it takes to restore network to normal operational condition.

A critical look at the chart (Fig. 4.4) shows that the average MTTR here is relatively low and almost constant for all fault types not minding the number of times such faults occur. The recommended duration by ITU of 4hrs MTTR is almost met here. Although, this fault types have no serious impact on call processing but affects specific services like: ‘’charging destination fault’’ and ‘’call limiting’’ which have serious impact on revenue and network quality of services; hence, their relative low MTTR values.

4.3 BAYESIAN MODELING OF BSS AND MSC DERIVED ERROR-LOG MESSAGE SUMMARY

A Bayesian network model has two components and is a pair: (D, H). ‘’D’’ is a Directed Acyclic Graph (DAG) whose edges represent direct dependencies between the variables i.e. the Causes and Symptoms as nodes and the elements of the qualitative aspect of the Model, while ‘’H’’ is a set of conditional probability functions; one for each variable and

this represents the quantitative aspect of the model. One specific feature of a mobile communications Fault Management Systems is that: a fault cause can result in a large set of similar symptoms, as there is no single fault assumption built into the process, hence, each possible explanation can be a conjunction of single cause.

Bayesian Networks are practically applied to model causal inferences systems where the modules of a system are modeled as the nodes of a BN, while the edges represent the cause-effect relationships between these elements. The qualitative part of a BN is encoded in the structure of the diagraph and the conditional probability distribution for the nodes encodes the quantitative structure. The Bayesian Model consists of two phases, Phase one is the qualitative aspect while phase two will encode the quantitative aspect.

4.3.1 QUALITATIVE MODELING OF NETWORK ELEMENTS ERROR- LOG MESSAGE SUMMARY USING SIMPLE BAYESIAN MODEL (FIRST PHASE)

A careful look at Appendix 2 (A and B) shows that for each fault cause, there are a number of symptoms that are logged at the NMC. The error log summary agrees with the assertion that a single fault cause results in a number of symptoms. This constitutes the first phase of our modeling (Fig.4.5). There are only two causes of fault symptoms at the BSS (Appendix 2A), i. e. Equipment and Transmission Network and each of this fault causes resulted in a number of symptoms (Fig. 4.5). This simple model helps a lot in drawing up commonalities between the faults which further takes us steps closer to the much desired well structured fault model for automatic diagnosis. Fig. 4.6 shows the Simple Bayesisn Model of the derived Error-log message at the MSC.

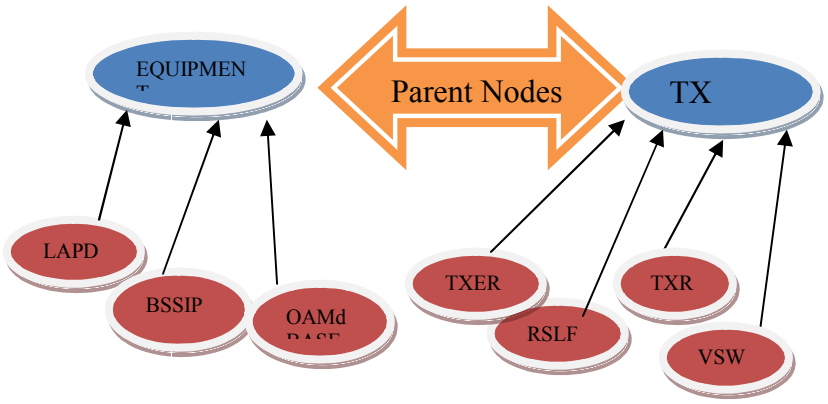


Fig 4.5 Simple Bayesian model of the BSS Faults (Error log-messages) Summary

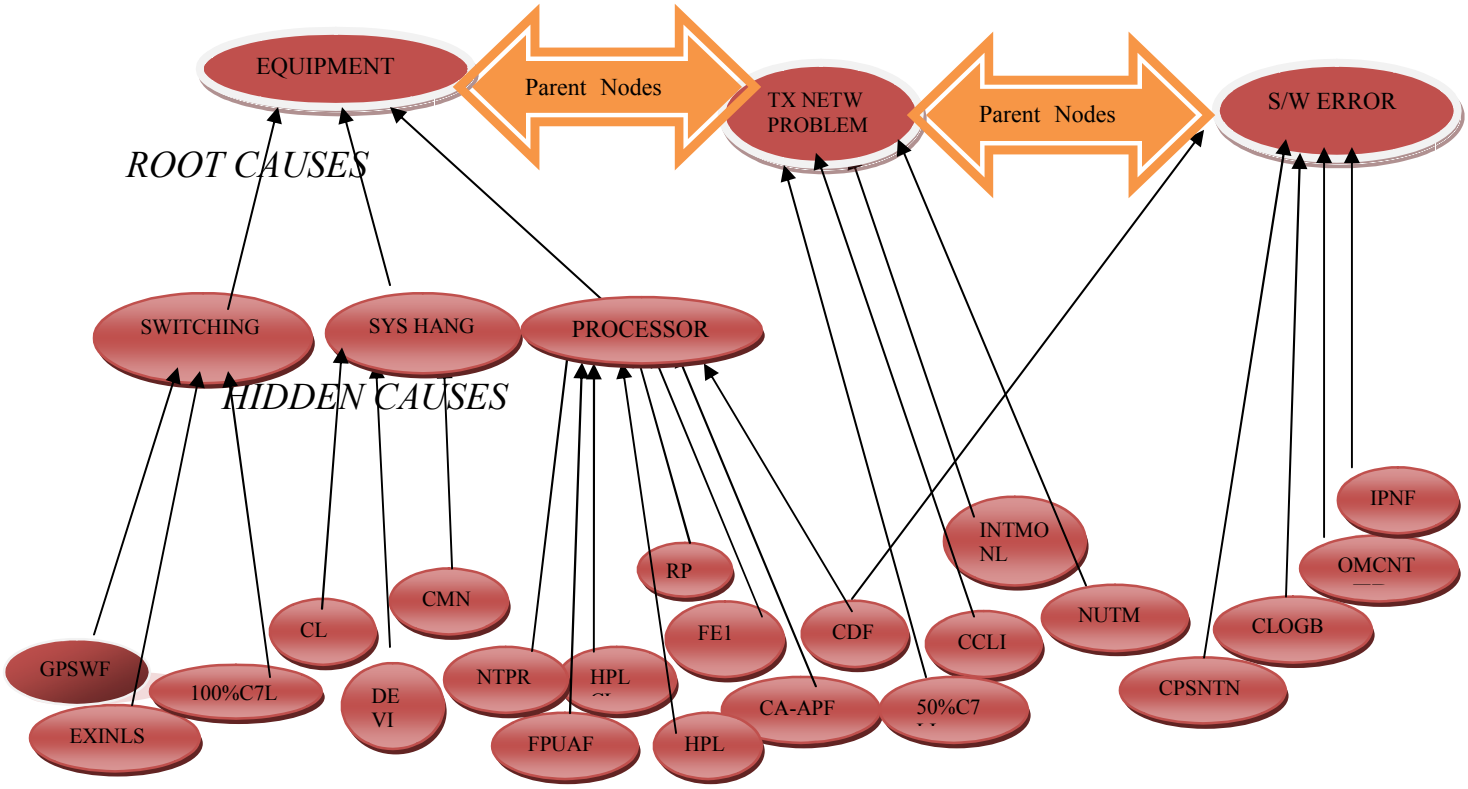


Fig 4.6 Simple Bayesian model of the MSC Faults (Error log-messages) Summary

To aid in the quest for an automated diagnosis of network alarm's fault management system; the Bayesian model can also be used to represent the faults occurring at the MSC

in a Diagraph. The fault types that were collected and filtered followed by correlation exercise are assigned new names i. e. they are masked. The alarm summary in Appendix 2B is in agreement with the fact that many fault types (symptoms) could be triggered by a number of causes or just a single cause.

A critical look at the table of Appendix 2B shows that there are three major causes of faults: Equipment (with all the hidden causes); Transmission network problems and Software error. Taking the causes and the symptoms as the elements of our Simple Bayesian Model gives the modeled fault tree for classified MSC Alarms shown in Fig. 4.6. This depicts the qualitative structural Bayesian model for MSC Fault summary. It is obvious from the representative model that the number of triggered alarms for a single cause is normally very high. In addition, the same alarms may be triggered by different cause. The Simple Bayesian Model helps to represent the well structured fault classes using the two most important elements in fault analysis which are the symptoms and their root causes.

4.3.2 QUANTITATIVE MODELING OF NETWORK ELEMENTS ERROR- LOG MESSAGE SUMMARY (SECOND PHASE)

The Bayesian network model has associated with it a Conditional Probability Table (CPT) that quantifies the effects that the parents have on the nodes depicting the quantitative aspect of the model. The graph as a whole, the conditional probabilities and the structure can be used to determine the marginal probabilities or likelihood of each node holding one of its states.

The second component (H) is a set of conditional probability functions, one for each variable (as Symptoms), that is:

$$= \{ \quad (\ / \ ) \ldots\ldots\ldots\ldots\ldots\ldots \{ \quad (\quad / \quad) \} \qquad (4.1)$$

This is equivalent to a unique joint probability distribution over U represented as:

$$(\ ) = \prod \quad (\quad / \quad) \qquad (4.2)$$

This constitutes the second phase of modeling which consists in defining the parameters for the CPT.

The required probabilities to completely define the model are:

1. *The prior probabilities, $P(C=C_k)$ for each fault causes C.*
2. *Conditional Probabilities of the Symptoms given the Causes, $P(S_i=S_{i,j} / C=C_k)$ for each state X.*

There are only two causes for all classes of faults in the BSS (Appendix 2A): Equipment and transmission, the probability $P(C=C_k) = 0.5$ was specified as uniform priors. A slight deviation from this assumption is necessary when a particular fault types occur many times before others are logged. Hence, the prior probability of caues for RSL (which occurs 1100 times out of 2096 error-logs) is slightly adjusted to 0.6. Also, there are three (3) causes for all fault types occurring at the MSC (Appendix 2B): Equipment, Transmission, & Software errors, with Twenty Six (26) symptoms in all and Equipment caused about 16 of such fault types as the dominant cause i.e. P(C1=16/26) = 0.6. The remaining Ten 10 symptoms were either caused by Transmission & S/W errors, i.e. P (C2= 10/26) = 0.4. This shows $\sum \quad = 1$, and since Bayesian modeling recommends the use of uniform priors, hence, the uniform prior of 0.5 P (C_k = 0.5) is used here as well.

The CPTs derived from the BSS and MSC alarm summaries are presented in Appendix 3 (A and B). The parent set of is = 2096, i.e. the total number of times error messages are logged and C_k = 0.5 for the BSS while the Parent set of is =6143 for the MSC. Refer to Appendix 3 A and B for the derived complete Conditional Probability Table distribution for both the BSC and MSC using the parameters defined thus far.

The systematic combination of the Structural model and numerical data of the overall fault (alarm) summaries for both BSS and MSC can now be realized in a Global Bayesian Network (GBN). The elements of the model are the Causes and Symptoms with the

parameters of the conditional probabilities as presented in Appendix 3. And the Global Bayesian Network derived in Fig 4.7 and 4.8.

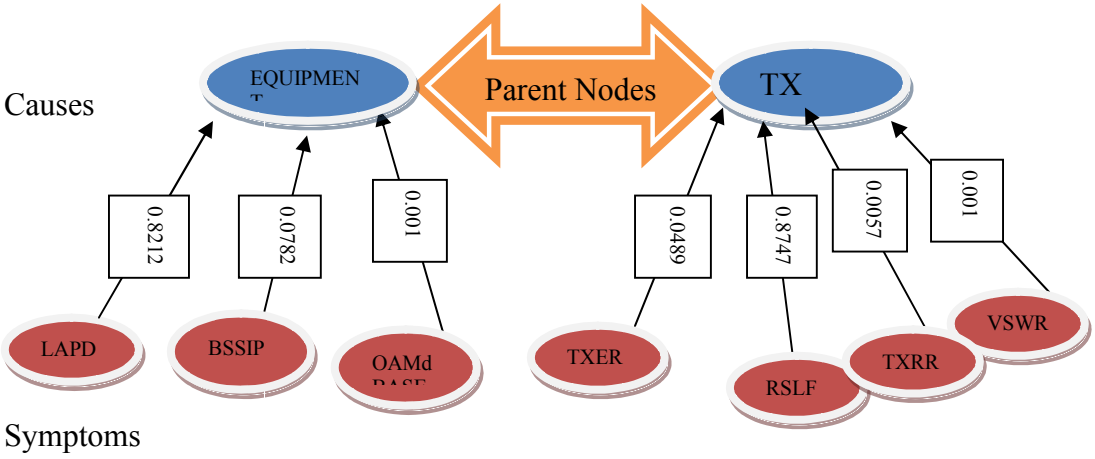


Fig. 4.7 Global Bayesian network model for BSS Error-Log Summary

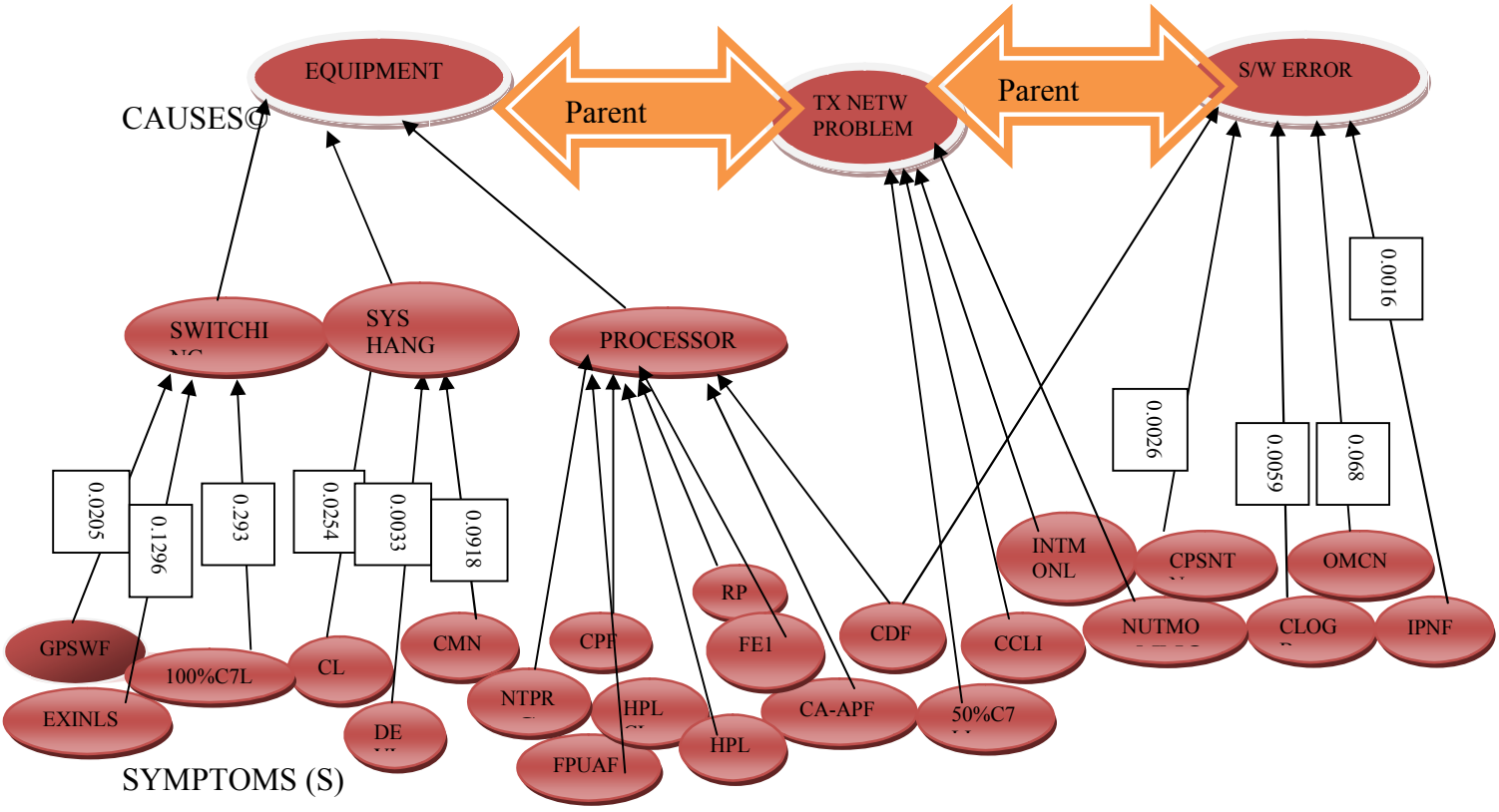


Fig. 4.8 Global Bayesian network model for MSC Error-Log Summary

4.3.2.1 INTERPRETATION OF RESULTS

The Global Bayesian Network model graphs or fault trees is considered to represent the joint probability distribution for all the variables as depicted (Fig. 4.7 and 4.8), each node has associated with it a conditional probability that quantifies the effects their parents (C) have on the nodes S. Taking the tree as a whole, the conditional probabilities and the structure can be used to determine the marginal probability or likelihood of each parent holding one of its states(S). This simply means that the Directed Acyclic graph (DAG) so derived is singly connected, each link is a bridge from symptom to root cause, where the change of one link leads to a different conditional probability due to new update and new faults will create an entirely new link.

Two components of the automatic diagnosis system may be distinguished: the model and the inference model. The model represents the knowledge on how the identification of fault causes is carried out given the symptoms; while the inference method is the algorithm that identifies the cause of the problems based on the value of the symptoms and the severity based on their value between 0 and 1as can be seen from the CPT (Appendix 3).

Talking about the Inference systems, there is causal inference (as in the Cause –effect phenomenon) and the diagnostic inference (using the BN Probabilistic modeling). The peculiar data in this case; thus serves as an Inference Algorithm which can be used to infer that:
P (X_j = x/E), represents the probability of a symptom X_j, being in certain state x, given the available evidence, E (cause), as a normalizing constant (thus informs the use of uniform priors P(C)). Off course, the target probability of the symptoms given the Cause is stated thus:
P (S_i=$S_{i,j}$ / C=C_k), which satisfies the unique joint probability function:

$$(\quad) = \qquad (\quad / \quad); \qquad \min 0, \quad \max 1$$

Now, if the product rule (from Baye's theorem), is applied to the sets of conditional probabilities, approximate values taken as 0 means the fault is almost non-existent and 1 is a case of constantly reoccurring multiple alarm for a particular error log message, e.g. RSL link failed with a target conditional probability of approximately 1.

As the value of the conditional probabilities varies from 0 to 1; the exact value is an indication of the severity of the particular fault type (Symptom). The Inference algorithm varies in much the same respect, they are either exact; approximate or heuristic values on singly or multiply connected graphs and are used for different inference task. The causes and symptoms for fault diagnosis can be modeled as random variables with two states: absent/ present; Off/On and as discrete random variables-[0,1]. It should be pointed out that since a random variable can only be in one of its finite states at a time, it is assumed that there is only one fault occurring at a time which is not always true in real life, hence the superiority of the Bayesian Inference diagnostic algorithm over Causal Inference Technique .

4.4 INTELLIGENT MANAGEMENT INFORMATION BASE (I- MIB) MATLAB SIMULATION FOR BAYESIAN INFERENCE USING THE VISUAL QUERRY BUILDER (VQB) GUI DATABASE TOOLKIT (PROPOSED)

In this work, using the Bayesian Inference technique method; one must be able to navigate among a number of Known Fault/Trouble Report (KF/TR) in a regular manner within a short period of time and as new updates are obtained. Hence, one critical issue is how to monitor dynamic updates to all these networks as error-log messages are received from Network Elements, thus triggering state changes in the nodes with inferences propagating throughout the network to be stored in an Intelligent Management Information Base (I-MIB).

In network operation, OSS and its components are implemented using Relational Database platforms like: Structured Query Language (SQL); Microsoft Access, Microsoft Excel, etc. The Database toolkits enables one to move stored data by Importing, Exporting and Updating of datas between Matlab and popular relational database platforms.

The database toolbox in MATLAB supports the import and export of data from any Open and Java Database Connectivity (ODBC/JDBC) compliant database management systems. The Database toolbox is a Java – based application, working in a windows environment like Microsoft Access or Microsoft Excel, there is the need to choose ODBC Driver for the Excel Files to interact with The Database Toolkit (Fig. 4.9).

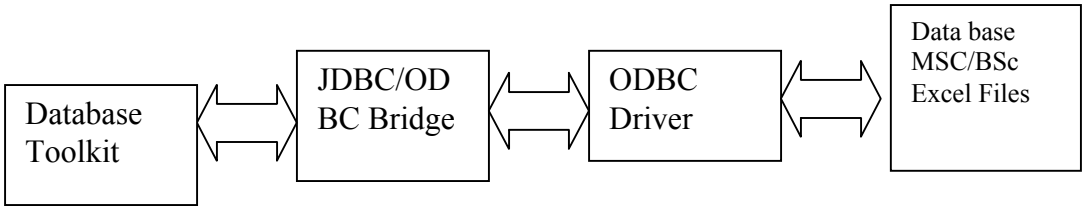


Fig. 4.9 Flow Chart showing the MATLAB Database ODBC/JDBC Connectivity with Database Directory Containing Error-Log Summary Files

4.4.1 SETTING UP A DATA SOURCE TO WORK WITH THE VQB

Before connection could be established with a Database from Matlab Database Toolkit, there is the need to set up a data source either from a Directory, Server, or a network name. Hence, from Matlab command window, enter ‘’querybuilder’’ command and the pop up window is displayed (Fig.4.10).

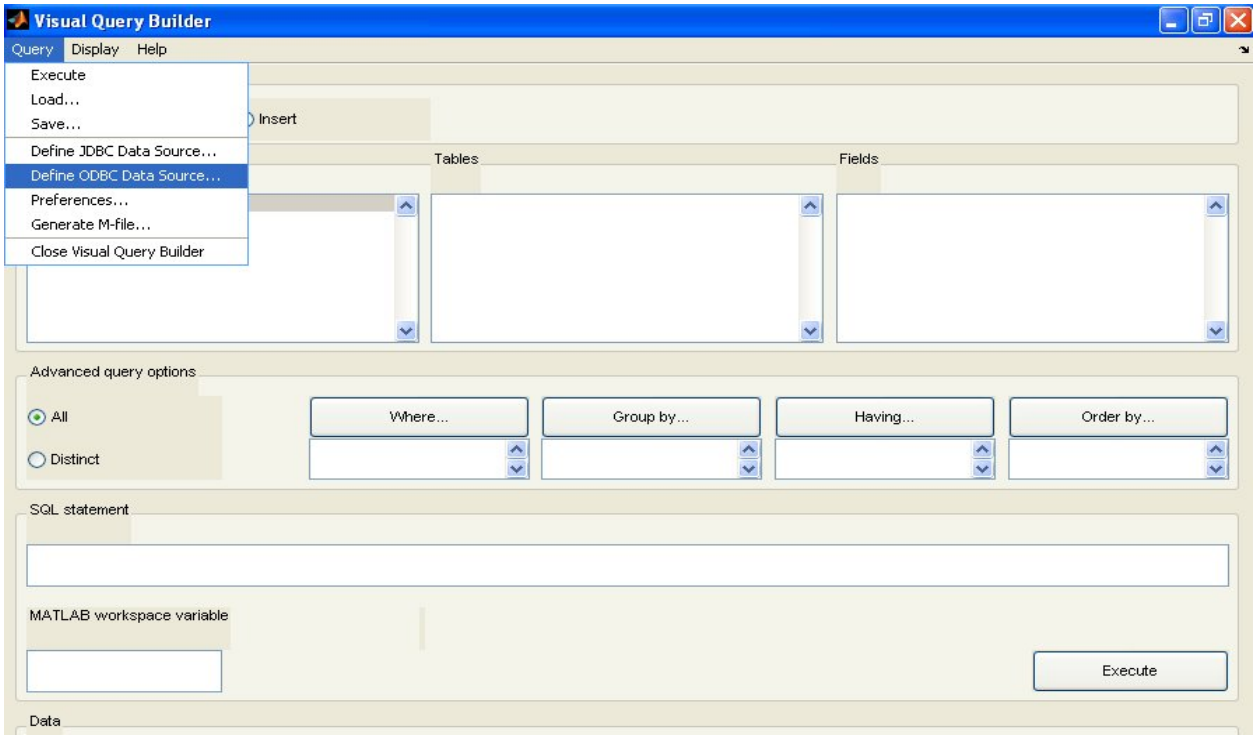


Fig. 4.10 Visual Query Builder Window

Check ‘’Querry’’ menu drop down, select ‘’Define ODBC Data Source’’ (Fig. 4.10). The data source resides on the local PC and it’s a windows platform which is ODBC Compliant, now select the driver for the database from the pop up window ‘’Create New Data Source’’(Fig. 4.11)

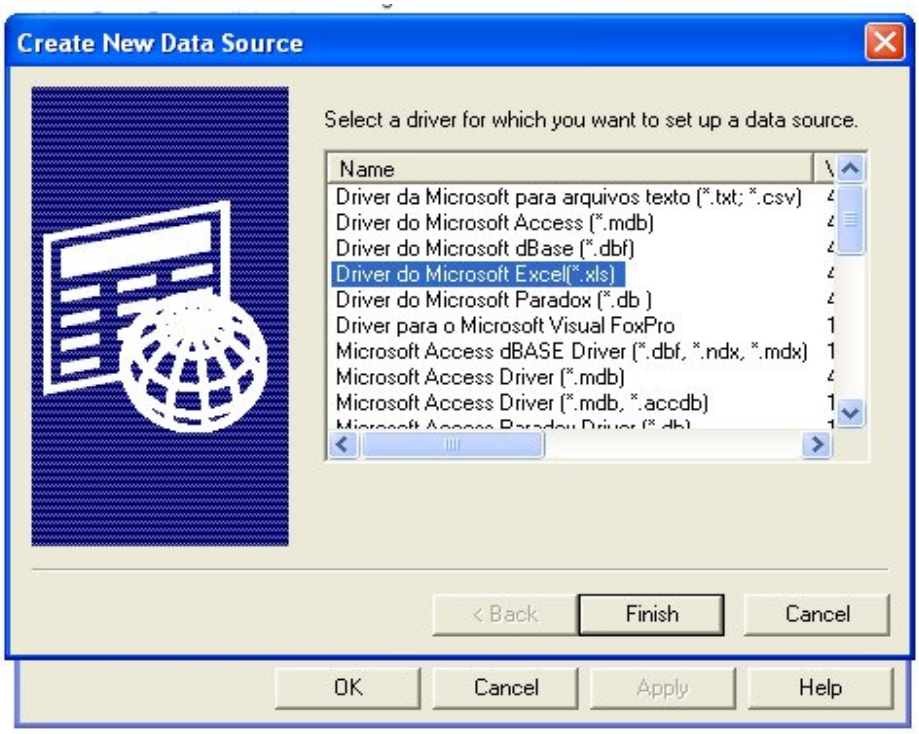
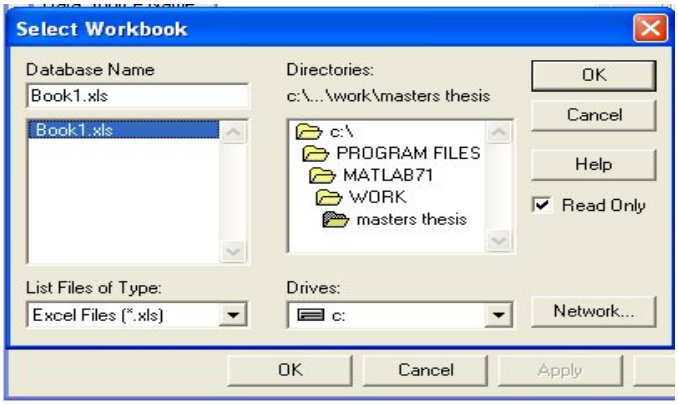


Fig. 4.11 Create New Data Source Window



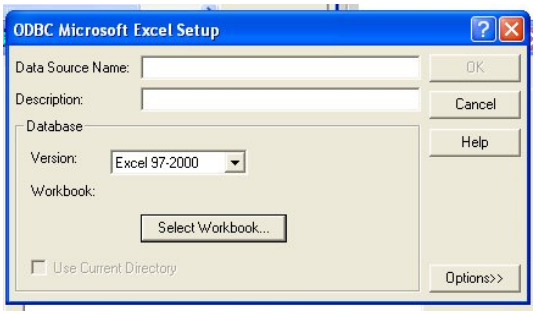


Fig. 4.12 (a) Database Directory path window *(b) ODBC workbook Excel setup Window*

On clicking ‘’Finish’’ the dialog box (Fig.4.12) appears for one to specify the database name, and path to the directory or network. The database name was set to ‘’Book1.xls’’ and saved in the Work Folder as ‘’masters thesis’’. If the file is in a remote location, then the path will be specified accordingly by clicking ‘’Network’’. Data Source Name is “NETWORK MANAGEMENT FAULTS’’ specified (Fig. 4.12 (b)). When done, Ok it and the following

“ODBC Data Source Administrator” Window appears showing data source saved as ‘’NETWORK MANAGEMENT FAULTS’’ (Fig 4.13)

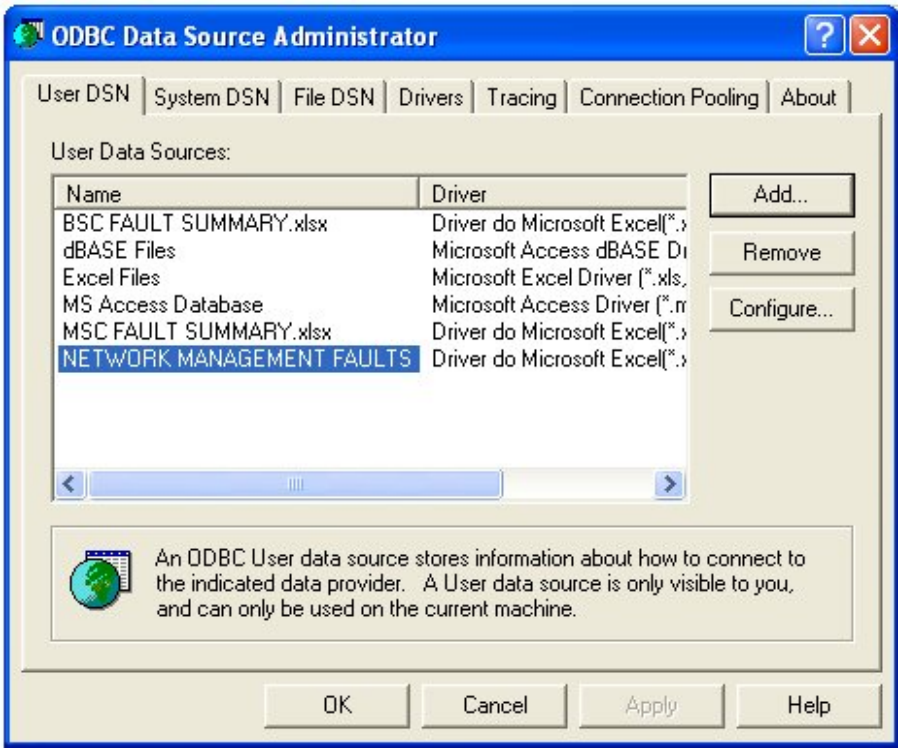


Fig. 4.13 ODBC Data Source Administrator” window

The “Add” feature could be used to add more files by following steps described so far. On clicking Ok, we are done with creating the ODBC Data Source (Fig. 4.13). We now used the “load” menu from Fig. 4.10 drop down menu. We could easily have entered “querybuilder” function from Matlab command window to load the database unto the VQB as well.

4.4.2 INTERPRETATION OF THE SIMULATED RESULT

Network Management Faults error -log summary in excel file has now been loaded as our data source with all the fields in the files from each table for both BSC and MSC. The “Advanced query options” was used to sort and group fields with specific conditions to be extracted for quick diagnosis in the VQB. The SQL statements are automatically generated and with Matlab Workspace variables specified accordingly as ‘’extractduration’’, when you “execute” (Fig. 4.14).

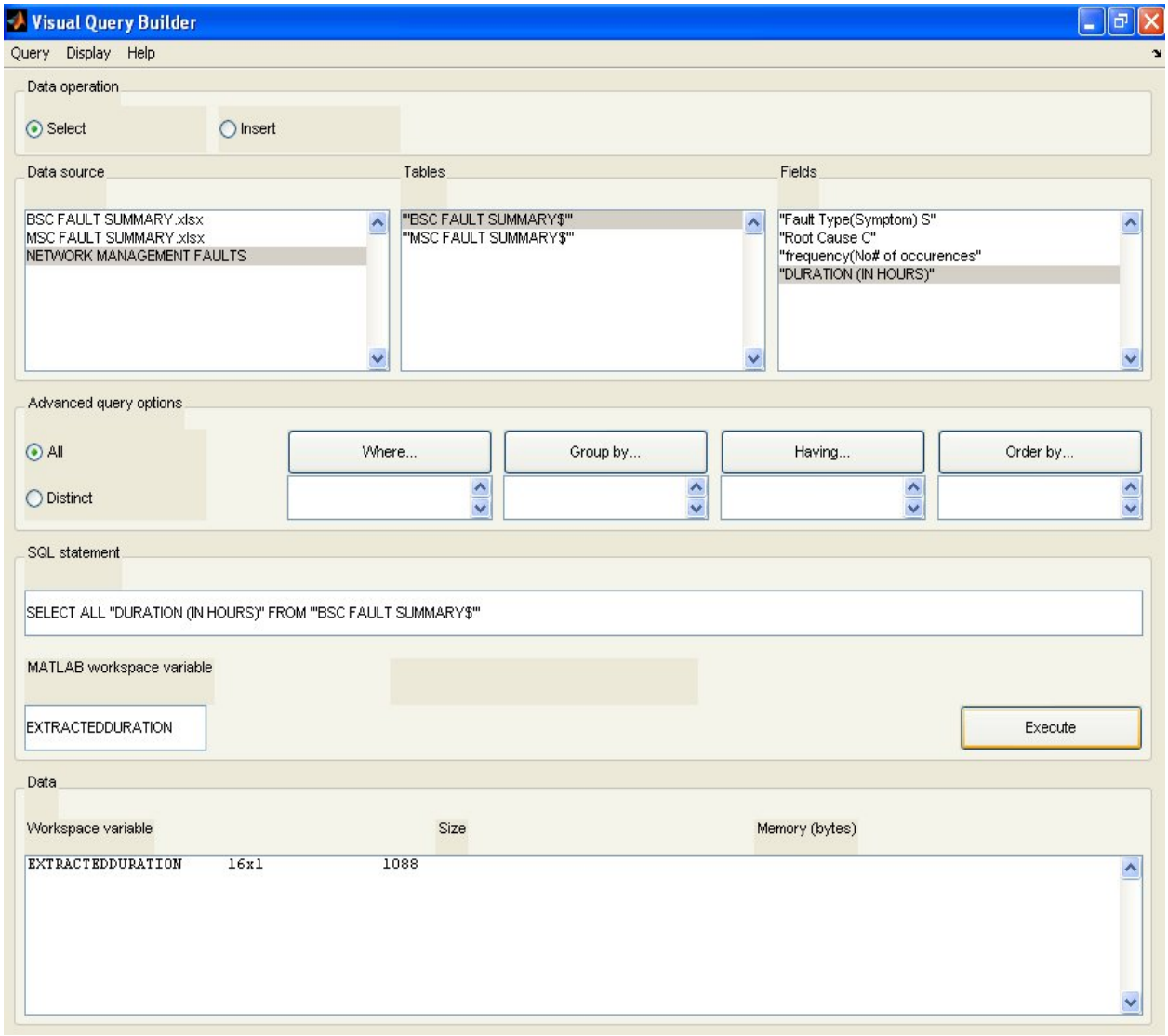


Fig. 4.14 Visual Query Builder Data operation and Execution pane

The "Extractedduration" is loaded unto the matlab Workspace and when opened, will be displayed in an Array Editor (Fig 4.15). All the fields defined in any of the NE files(Tables) could be loaded unto the Array Editor and new updates could be loaded as well, using the quick "insert" feature of the VQB. With this extracted array field, we were able to create a database of the fault summaries. One could also extract more than one field and it is possible to use this

VQB's Advanced Query options (Fig. 4.14): ''Where''; ''group by''; ''having''; ''order by'' to specify conditions for each cell arrays to be extracted.

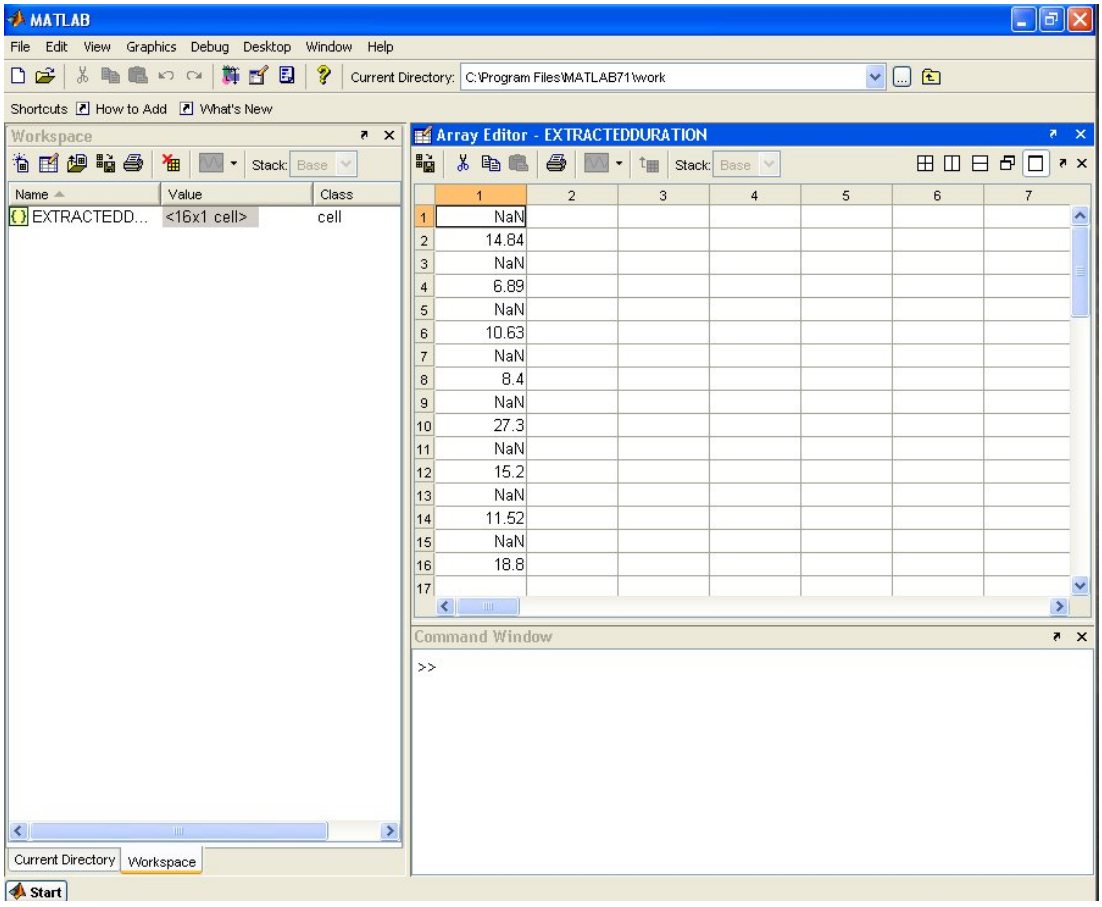


Fig 4.15 Matlab Extracted Field on Array Editor

The Visual Query Builder (VQB), which comes with the Database Toolbox, is an easy-to-use Graphical User Interface (GUI) for exchanging data with the database. One can use the VQB instead of functions or in addition to using Database Toolbox functions. With the VQB, you retrieve data by selecting information from lists to build queries. The VQB imports the data into the MATLAB workspace one could then can process the data using the MATLAB suite of functions. With the VQB, we were able to load and display the retrieved information in relational tables, reports, and charts. Hence, it can be used in advanced sorting of raw error log messages collected at the NMC using any of the Database platforms.

Although the fault trend analysis which has actually helped in analyzing network parameters that affects overall performance of the GSM/GPRS systems would have been made a lot easier but still inadequate in that Bayesian modeling is more of Probability Belief Network. Finally, the VQB makes the proposed Relational Database Systems realizable because of the absolute need to store all possible combinations of states between sets of related parents (Causes) and Child (Symptoms) nodes.

CHAPTER FIVE

CONCLUSIONS AND SUGGESTIONS FOR FURTHER WORK

5.1 Significance of the Study

The instance of a fault can cause numerous alarm events to be generated from an individual network element i.e. alarms are often interrelated upstream and downstream. Correlation and Filtering serves to diminish the number of alarms presented to the operator. Ideally, the process should be able to facilitate fault prediction, identification and diagnosis. Behavior prediction warn operator before hand of severe faults from the alarms that are presenting themselves. The Bayesian paradigm and its extensions offer the machinery to achieve these ideals. Although methods such as Artificial Neural Networks have proven to obtain good predictive performance, they do not meet one important goal of ‘’comprehensibility and reliability’’. Hence Telecommunications companies do not wish to install black boxes into their FM System.

Bayesian Network’s graphical modeled structures and probabilistic inference systems more than meet the need for reliability and comprehensibility. In order to handle all these different tasks, some techniques are utilized for explicitly modeling the Mobile network management system and its behavior, and for utilizing knowledge-based reasoning and an intelligent system to perform proactive and reactive reasoning on the FM models.

The proactive mode is initially effective for those faults that are well known i.e. have a precise fault model, being part of well modeled fault scenarios, having intermediate symptoms but also applies to new faults.

Machine learning is still in its infancy in addressing real-world problems; Machine learning for data classification and interpretation requires the compilation of libraries of fault patterns for the performance of Network Devices. These libraries do not always provide knowledge-rich structures or justifications for device behavior or failure.

Downtime in a network not only results in loss of revenue but can lead to serious contractual penalties. It is therefore not surprising that network operators are extremely keen to remedy faults as quickly as possible. To this end, not only is fault identification critical but an estimation of a fault's lifespan would greatly assist in managing and assessing maintenance strategies. Fault Management Event/Alarm is an important but difficult area of telecoms network management. Networks produce large amounts of alarm information that must be analyzed and interpreted before the faults can be properly diagnosed.

5.2 Limitations

The following limitations were encountered during the course of this work and assumptions made where necessary:

1. *The Fault trend analysis was based on an assumption that there can be only one fault occurring at a time; which is not possible in real time network.*
2. *Meanwhile, if the number of the symptoms becomes too large, basing such a model on some conditional probability is tedious because obtaining samples of the Prior is often easy and the Posterior is more difficult i.e. from Bayesian theorem (Prior x Likelohood = Posterior x Evidence).*

3. *During network operation; event/alarms have direct impact on Key Performance Indicators (KPIs) and they both affect network performance on the whole, but this study is based on only network software alarms.*
4. *Sourcing information for referencing and enrichment of the research was not that easy since few researches had been conducted in the field of automatic diagnostic fault management system.*
5. *Contrary to other application domain; there is usually no database of classified faults and no Of-The-Shelf software which simulates the Cause and Effects (symptoms) ideally, a network operator should grant access to the NMS error log-messages regularly for everyday troubleshooting experts to carryout periodic analysis and once the faults are resolved save the causes/symptoms (a case is a set of parameters for some symptoms together with the actual causes).*

5.3 Summary of Findings

1. *The results of the Fault Trend Analysis show that there are two important parameters that affect network performance during network event/alarm analysis: "The Frequency of Occurrence" of the fault types (symptoms) from a given cause; and the "Mean Time to Clear such faults (MTTR) or duration.*
2. *The fault trend analysis shows that the higher the frequency of occurrence of any particular fault types the lower the duration or the mean time to clear such faults and vice versa. But, a deviation from this observation was noticed for those faults at the MSC that have little or no impact on signal processing.*
3. *In mobile network operations, the fact that a single fault cause can result in a number of symptoms, and the same alarms may be triggered by different causes; has been validated by the Simple Bayesian Model from the derived error-log message summary.*

4. *The Bayesian Network model consists of two components; Qualitative and Quantitative parts that is realized here in both the First and second phases of the modeling respectively.*
5. *Combining explicitly the parameters of the numeric quantitative aspect and the elements of the qualitative aspect (causes and symptoms) of the model in a Global Bayesian Network, gives the representative Directed Acyclic Graph showing the causal chains to supply evidence of past event to see what the most likely cause of future errors might be.*
6. *Because of the need to store all possible combinations of states between sets of related parent (cause) and child(symptom) nodes; an Intelligent Management Information Base (I-MIB) MATLAB) simulation of the derived error log message using the Visual Query Builder GUI database tool was proposed to mimic the relational database deployed in the industry.*

5.5 Conclusions

7. *Systems that are subject to uncertainty in their behavior are often modeled by Bayesian Networks. That is why parameters like: the fault types (Symptoms); Root causes; and the time that observed error- logs are registered and the time they are resolved referred herein as MTTR (duration) are suitable as important elements in analyzing the impact of faults on GSM/GPRS network performance. These parameters can significantly affect the formulation of hypothesis for future fault prediction derived from a well structured fault model. Such systems enable Mobile Network operators to face the challenges of increasing complexity of Fault Management Systems for current and future Network Management Systems.*

The Bayesian global network can be used for deduction in the field of Network Fault Management domain, given alarm datas; it can help to determine the most probable cause (s) of the alarm symptoms and also the seriousness of the effect of the individual symptom. The conditional probabilities of the symptoms given the cause enable the system to act as an Expert systems being both reactive and proactive in the real sense, though not yet predictive.

One critical issue is how analyst will be able to monitor dynamic updates to all these networks as messages are received from Network Elements, thus triggering state changes in the nodes with inferences propagated throughout the network.

Those parameters may be either elicited by experts in the NMS or calculated based on statistics gathered for fault management analysis. This is the reason why the model has to be based on knowledge, i.e. experts defined model parameters. When the number of parameters to be set is large, which is normally the case, inaccuracies in setting these parameters is unavoidable. Although, probabilistic reasoning may not be exact to be useful and network operators are not interested in deploying Artificial Neural networks to predict faults; Bayesian networks subsume neural networks, the usefulness of Bayesian reasoning and the proposed I- MIB cannot be overemphasized. Hence, the aim of this paper to propose methods namely: Bayesian Model (BM); I-MIB MATLAB simulation, which overcomes the effects of inaccurate model parameters, for easy and quick troubleshooting of network faults in order to enhance the diagnosis accuracy, has been realized to a great extent thus far.

5.4 Recommendations for Further Work

1. *To lay a better foundation for the integrated mobile network management system, research should be directed at deploying Artificial Intelligent (AI) techniques like: Fuzzy Causal Probabilistic Network (FCPN). If an alarm vector belonging to an initial cause is known, the neural network can be trained to transform the initial vector into an initial cause.*

2. *The computational challenge in making Bayesian model work is computing the Posterior probability, we have so far been able to resolve the prior and likelihood probabilities for the derived summary of error log messages; efforts should now be concentrated on resolving the posterior i.e. (likelihood x prior = posterior x evidence) of the Bayesian theorem proposition. This could be useful in predictive systems of the future rather than the mostly reactive and proactive systems of today.*

3. *The large volume of data (raw error-log messages) collected real time during network operation could be fed directly into MATLAB Database tool- Visual Query Builder (VQB) to automatically build query for selecting or filtering during analysis. One can now represent the derived summary in charts and graphs using MATLAB Suit of functions to do the analysis and modelling of software error parameters.*

REFERENCES

Aldrich, A. and Stephen, E. (2008). *Bayes' Theorem: Bayesian Analysis of Analytic Frequentis Probability and Frequentis Statistics. J. Newman Publishers. Milano. 255(5), 97-131.*

Baras, J. S. and Mykoniatis, H. G. (1998, April 3). Integrated Distributed Fault Management for Communications Networks. *Technical Report, CSHCN TR 98 – 10, p. 1 – 4.*

Binay, S. and Masum, H. (1999, May 1). A conceptual framework for network management event correlation and filtering systems. *IEEE/IFIP Intonation conference on Integrated Network Management Bombay*. Retrieved November 5, 2010 from http://www.iee.org/

Boix, C. and Svedberg, M. (2008). Model based Alarm Coordination system for primary and secondary alarm notifications. *Verizon business network services Inc., Patentdocs, Arlighton, VA, USA. Retrieved January 20, 2011 from Patendocs database.*

Boutabu, R. and Dovik, S. (2000, April 5). Software fault management system. *Expert systems for Communications Network, US patent, Application No. 081918100. p. 20. Retrieved October 15, 2010, from patentdocs database.*

Bradey, J. (1994). Dynamic belief networks for discrete monitoring. *IEEE Trans. On Systems, Man Cybernetics. 34(11), 1593- 1610.*

.

Carls, G., Nedil, W., Tuchis, K. (1997). Using neural networks for alarm correlation in cellular phone networks. *In Proceeding of the IEEE International Workshop on applications of Neural Networks to Telecommunications, Melbourne, Australia*

Clement, L. M. and John B. G. (1980). Software Quality Assurance: Testing and Validation. *IEEE Trans. Software Eng. 68(9), 1160-1169.*

Cooper, G. (1990). The Computational complexity of probabilistic inference using belief Networks. *In proceeding of IEEE on Artificial Intelligence, Milano. 42(10), 393 – 405.*

Daniel, F. (2005). Internet Telephony: NMS Communication, [Press release]. *Califonia: NMS Communications limited.*

Daniel, P. and Tsao, M. (1983). Trend analysis on systems error profiles. *In IEEE Proceedings & Symposium on Fault Tolerant Computing, Milano, Italy*. p. 116-119.

David, M. (2007). Nortel Units Performance Management Solutions. *Nexus Telecoms Whitepaper, Document T – 12 – 00247, Nexus Switzerland. Retrieved June 1, 2010 from* http://www.nexus.com/nortelunits/performance

Dereviere, Van M. and Verbuas, J. (2003). Common GSM software components. *Alactel Telecommunications Review*. 21(1), 124-128.

Distaso, J. (1980). The measurement and management of software reliability. *IEEE Trans Software eng. 68(9), 1133-1134.*

FCAPS network management functional model. (2007). *Retrieved November 10, 2010. From* http://www.itu.int/*SpecificationDocument/M.3000/M.34000.html*

Frolich, P., Jobmann, K. and Nejdl, W. (1997). Model based alarm correlation in cellular phone networks. *In Proceedings of IEEE International Workshop on Modelling, Analysis, and Simulation of Computer/Telecommunications Systems, Haifa, p. 1-4.*

Glosssoler, S. A. (1978). The DACS glossary – A Biblography of software engineering terms. *Data analysis center for software Rep. Gloss-1, Rome Air Development.*

Hawkins, B. E., Jim, N. R., Kenny, M., and Taylor, P. (2009). Outage Analysis System. *Verizon Business Network services Inc., Patentdocs, Arlighton, VA, USA. Retrieved January 20, 2011 from Patendocs database.*

Herman, W., Klaus-Dieter, T., Petere, F. and Sebastian, S. (1997). Using Neural Networks for alarm correlation in Cellular Phone Networks. *In Proceedings of the IEEE international workshop on applications of Neural Networks to Telecommunications, Stocholms, Sweden*. Retrieved October 26, 2010 from http://www.iee.org/

Hughes, S. (2006). Enterprise architecture for next generation telecommunications service provider. *Huges Technical Journal*. Retrieved October 12, 2010 from http://www.hsc.com/

Jack, D. (1980). Software Management: A Survey of the Practice. *IEEE Trans. Software Eng. 68(5), 1103 – 1119.*

Jacobson, G. and Weissman, M. D. (1993, November 10). Alarm Correlation Techniques. *IEEE network forum, Stuttgart, Germany*. 7(6), 52-59.

Jaynes, E. (2003). Probability Theory: The Logic of Science. *Cambridge University Press, ISBN 0-521-59271-2. Retrieved November 15, 2009 from Cambridge press database.*

John, B. and Clement, L. (1980). Software Quality Assurance: Testing and Validation. *IEEE Trans: Software Eng. 68(9), 1154-1150.*

John, W. S. and Williams, R. (1996). Improving the accuracy of diagnostic provided by fault dictionaries. *Proceding of the 14th IEEE VLSI Test Symposium, CA*. Retrieved January 20, 2011 from http://www.iee.org/

Karmouch, A. and Pharm, V.(1998. July 16). *An overview of Mobile Software Agents*. Paper presented at the University of Ottawa, Canada. Retrieved June 14, 2009 from IEEE Communications Magazine.

Lauritzen, L. and Spiegelhalter, D. (1998). Local computations with probabilities on graphical structures and their applicationa to expert systems. *J. R. Statistic Soc. B. Malaga, Spain. 50 (2), 157 – 224.*

Liu, G. and Yang, E. J. (1999). Composite Events for Network Event Correlation. *IEEEE/IFIP International symposium on Integrated Network Management, South Korea. Retrieved June 20, 2010 from http://www.ieee.com/compositeevent.*

Lucien, Le Cam. (1986). Asymptotic Methods in Statistical Decision Theory. *Von muses and Barstein Press, Paris. 3(1), 1-5.*

Masud, A. (2006). Fault Management in Communications Networks. *MSC Thesis. Ahmadu Bello University, Zaria. Retrieved January 7, 2009, from Electrical Engineering departmental library.*

Mathew, C. (2004). System and Method to locate and correct software errors within a protocol stack for wireless devices. *Retrieved January 15, 2010 from Braod Com Texas Corporation Technical database.*

Maye, J. and Morvan, G. (2006). Achieving efficient operational transformation. *Alactel telecommunications review*. 21(3), 253-255.

Nicolas, M., and Peirce–Nenri, G. (2003). Integrated network and service management for Mobile Network. *Alcatel telecommunication review*. 10(4), 153-157.

Oliver A. J. and Sahoo, R. K. (2002). Critical event prediction for proactive Network Management. *The 9th Tokyo ACM SIGKDI International Conference on Knowledge Discovery and Data Mining, p. 426 – 435.*

Oroge, C. O. (1991). Fundamentals of reliability and testing methods. *Sooji press limited. Kaduna, p. 9-14.*

Paessler, M. (2007). Towards a common OSS Architecture. *A Journal on Open Element Management System (EMS) Suite by Nokia. Retrieved January 10, 2010 from* www.nokiasiemensnetworks.com/

Riverrol, C. and Sanctis, C, (2005). Improving Adaptive Network-based Fuzzy Inference Systems (ANFIS): A practical approach. *Asian journal of Information Technology.* 4 (12), 1208-1213.

Richard, T. (2001). Algebra of probable inference. *The John Hopkins University Press. 12(4), 97 – 98.*

Shewzen, P. (2003). Base station subsystem of CDMA Cellular Mobile Communication System. *Technical manual (V.53) [Brochure]. ZTE Corporation, Shengzen, China.*

Towell, G. and Shavlik, S. (1994). Knowledge based Artificial Neural Networks: Artificial Intelligence. *Journal of computing.* 70(2), p.119-166.

Wallstrom, M. (2007). Automation of Mobile Radio Network Performance and Fault Management. *MSC Thesis, Helsinki University of Technology. Retrieved June 7, 2010 from the Department of Electrical Engineering online database.*

Wendel, O. (2009). Network Management System: Best Practices Whitepaper. *Document ID: 1 5114.Retrieved November 5, 2010 from Cisco Systems database.*

Wietgrafe, H. (2002). Investigation and practical assesment of alarm correlation method in GSM Network Management'', *In proceeding of the IEEE/IFIP Network Operations and Management symposium. Florence, Italy.*

Yang, C. (1997). Fuzzy Bayesian Inference. *In proceedings of the IEEE international Conference on systems, man and cybernetics at Orlando, Florida. Retrieved October 12, 2010 from http://www.iee.org/bayesianinference/*

APPENDICES

APPENDIX 1

(A) MSC ERROR LOGS TO BE FILTERED AND CORRELATED (SAMPLE)

Status	Trouble Ticket ID	Region	Impacted	Fault Type	Duration	Root Cause	Resolution Method	Solution Remarks	Dispatch To	Group Type
Closed	TT0000000096021	Lagos	LGHLR05	SIZE ALTERATION OF DATA FILES SIZE CHANGE REQUIRED	0 Days 2 Hours 3 Min 0 Sec	Equipment	Reset System	The data block increased on the node	JOEY	MSC
Closed	TT0000000096586	Lagos	LAMSC03	High Processor Load and Call limiting		Equipment	Congestion Cleared	Congetion cleared by itself	Peter Igwiloh	MSC
Closed	TT0000000096587			High Processor Load and Call limiting		Equipment	Congestion Cleared	Congetion cleared by itself	Peter Igwiloh	MSC
Closed	TT0000000096588	Lagos	LAMSC12	High Processor Load and Call limiting		Equipment	Congestion Cleared	Congetion cleared by itself	Peter Igwiloh	MSC
Closed	TT0000000096589	Lagos	LGTSC01	High Processor Load and Call limiting		Equipment	Congestion Cleared	Congetion cleared by itself	Peter Igwiloh	MSC
Closed	TT0000000096590	Lagos	LAMSC07	High Processor Load and Call limiting		Equipment	Congestion Cleared	Congetion cleared by itself	Peter Igwiloh	MSC
Closed	TT0000000096785	Lagos	LAMSC08	SIZE ALTERATION OF DATA FILES SIZE CHANGE REQUIRED	0 Days 16 Hours 55 Min 23 Sec	Database Change Completed	Data size increased by the NMC.	Niran		
Closed	TT0000000096786	Lagos	LAMSC11	SIZE ALTERATION OF DATA FILES SIZE CHANGE REQUIRED	0 Days 16 Hours 58 Min 23 Sec	Database Change Completed	Data size increased by the NMC.	Niran		
Closed	TT0000000096793	Lagos	LAMSC11	High processor load and call limting	0 Days 2 Hours 19 Min 0 Sec	Equipment	Cleared itself	Niran could not be reached on phone	Peter Igwiloh	MSC

Closed	TT0000000096795	Lagos	LAMSC04	High processor load and call limiting	0 Days 2 Hours 19 Min 0 Sec	Equipment	Cleared itself	Niran could not be reached on phone	Peter Igwiloh	MSC
Closed	TT0000000096796	Lagos	LAMSC09	High processor load and call limiting	0 Days 2 Hours 19 Min 0 Sec	Equipment	Cleared itself	Niran could not be reached on phone	Peter Igwiloh	MSC
Closed	TT0000000096798	Lagos	LAMSC10	High processor load and call limiting	0 Days 2 Hours 41 Min 10 Sec	Equipment	Cleared itself	High processor load and call limiting cleared. Congestion cleared itself	Peter Igwiloh	MSC
Closed	TT0000000096799	South East	ASMSC01	High processor load and call limiting	0 Days 2 Hours 19 Min 0 Sec	Equipment	Cleared itself	Niran could not be reached on phone	Johnson	MSC
Closed	TT0000000096800	South South	PHMSC01	High processor load and call limiting	0 Days 2 Hours 19 Min 0 Sec	Equipment	Cleared itself	Niran could not be reached on phone	Eniola	MSC
Closed	TT0000000096801	Lagos	LAMSC08	High processor load and call limitng	0 Days 2 Hours 19 Min 0 Sec	Equipment	Cleared itself	Niran could not be reached on phone	Peter Igwiloh	MSC
Closed	TT0000000096802	South East	ASMSC01	SIZE ALTERATION OF DATA FILES SIZE CHANGE REQUIRED	0 Days 14 Hours 17 Min 45 Sec	Database Change Completed	Data size increased by the NMC.	Niran		
Closed	TT0000000096803	Lagos	LAMSC10	SIZE ALTERATION OF DATA FILES SIZE CHANGE REQUIRED	2 Days 3 Hours 47 Min 45 Sec	Database Change Completed	NI increased.	Niran		
Closed	TT0000000096950	South East	ASMSC01	High processor load	0 Days 1 Hour 47 Min 36 Sec	Equipment	Congestion Cleared	Congestion Cleared	Johnson	MSC
Closed	TT0000000096951	Lagos	LAMSC04	High processor load		Equipment	Congestion Cleared	Congestion Cleared	Chibuzor	MSC
Closed	TT0000000096952	Lagos	LAMSC10	High processor load		Equipment	Congestion Cleared	Congestion Cleared	Chibuzor	MSC
Closed	TT0000000096953	Lagos	LAMSC09	High processor load		Equipment	Congestion Cleared	Congestion Cleared	Chibuzor	MSC
Closed	TT0000000096954	Lagos	LAMSC11	High processor load		Equipment	Congestion Cleared	Congestion Cleared	Chibuzor	MSC
Closed	TT0000000096963			Planned work	30 Days 10 Hours 9	Maintenance .	Planned work	Folorunsho		

					Min 45 Sec		completed			
Closed	TT0000000096968			Cannot monitor node	0 Days 1 Hour 27 Min 20 Sec	Equipment	Reset System	The node was rebooted. Info by Momoh.	Momoh	MSC
Closed	TT0000000097097	South East	ASMSC01	Canot monitor	0 Days 0 Hours 23 Min 11 Sec	Generator	GCLK Resync	Power successfully changed over between the two generators at Ogbere BB.	Johnson	MSC
Closed	TT0000000097098	South South	PHMSC01	Canot monitor	0 Days 0 Hours 23 Min 11 Sec	Generator	GCLK Resync	Power successfully changed over between the two generators at Ogbere BB.	Johnson	MSC
Closed	TT0000000097099	South South	PHMSC02	Canot monitor	0 Days 0 Hours 23 Min 11 Sec	Generator	GCLK Resync	Power successfully changed over between the two generators at Ogbere BB.	Johnson	MSC
Closed	TT0000000097100	Central	ABMSC01	Canot monitor	0 Days 0 Hours 23 Min 11 Sec	Generator	GCLK Resync	Power successfully changed over between the two generators at Ogbere BB.	Johnson	MSC
Closed	TT0000000097101	Central	ABMSC02	Cannot monitor	0 Days 0 Hours 23 Min 11 Sec	Generator	GCLK Resync	Power successfully changed over between the two generators at Ogbere BB.	Johnson	MSC
Closed	TT0000000097102	North West	KDMSC01	Canot monitor	0 Days 0 Hours 23 Min 11 Sec	Generator	GCLK Resync	Power successfully changed over between the two generators at Ogbere BB.	Johnson	MSC
Closed	TT0000000097103	North West	KDMSC02	Canot monitor	0 Days 0 Hours 23 Min 11 Sec	Generator	GCLK Resync	Power successfully changed over between the two generators at Ogbere	Johnson	MSC

								BB.		
Closed	TT0000000097112	South East	ASMSC01	100% C7 link failure	0 Days 0 Hours 23 Min 11 Sec	Generator	GCLK Resync	Power successfully changed over between the two generators at Ogbere BB.	Johnson	MSC

(B) BSC ERROR LOGS TO BE FILTERED AND CORRELATED (SAMPLE)

Status	Trouble Ticket ID	Region	Impacted	Fault Type	Duration	Root Cause	Resolution Method	Dispatch To	Group Type
Assigned	TT0000000061801	Lagos	414_CANAAN_LAND	GENERATOR FAULT				Enato	BTS
Closed	TT0000000061802	Lagos	771_SANGO_OTA	GENERATOR FAULT	4 Days 0 Hours 26 Min 0 Sec	Generator	GENERATOR RESTART	Enato	BTS
Resolved	TT0000000063283	Lagos	240_AKUTE	GENERATOR FAULT	2 Days 12 Hours 35 Min 0 Sec	Generator	GENERATOR RESTART	Bayo	BTS
Closed	TT0000000083204	North West	KAD054	LAPD_OML failure	0 Days 1 Hour 26 Min 41 Sec	Transmission	Cleared itself	Emmanuel	BTS
Assigned	TT0000000086352	Lagos	137_EXQ_PLAZA	HIGH TEMP				OBASI	BTS
Assigned	TT0000000089124	Lagos	055_SANGO_OTA	HIGH TEMP				AYOOLA	BTS
Closed	TT0000000093696			HIGH TEMP	0 Days 10 Hours 45 Min 0 Sec	Cascade Site	GENERATOR RESTART	Abel	BTS
Closed	TT0000000094248	Lagos	292_IBA	cascaded	0 Days 7 Hours 1 Min 0 Sec	Cascade Site	GENERATOR RESTART	Sola	BTS
Closed	TT0000000096538	Lagos	967_KETU	cascaded	0 Days 0 Hours 45 Min 0 Sec	Cascade Site	Power restored	BOLA	BTS
Closed	TT0000000096591	North East	BOR106	LAPD_OML failure		Equipment	Replaced Equipment	Tony	BTS
Closed	TT0000000096594	Central	TAR100	LAPD_OML failure		Cascade Site	GENERATOR RESTART	Yahaya	BTS
Closed	TT0000000096595	Central	TAR105	LAPD_OML failure		Generator	GENERATOR RESTART	Yahaya	BTS
Closed	TT0000000096596	Central	TAR109	LAPD_OML failure		Cascade Site	GENERATOR RESTART	Yahaya	BTS
Closed	TT0000000096597	Central	TAR108	LAPD_OML failure		Cascade Site	GENERATOR RESTART	Yahaya	BTS
Closed	TT0000000096598	South South	18-OPOBO_RD_OGBORHILL_New	RSL link Failed	1 Day 11 Hours 1 Min 0 Sec	Generator	GENERATOR RESTART	Adeniyi Babafemi	BTS
Closed	TT0000000096599	North West	KAD007	LAPD_OML failure		Generator	GENERATOR RESTART	Gana	BTS

Closed	TT0000000096602	South East	50-NRI	RSL link Failed	0 Days 7 Hours 50 Min 0 Sec	Transmission	Cleared itself	Fidelis	BTS
Closed	TT0000000096603	South South	3-CHINDA_EST	GENERATOR FAILURE TO START	0 Days 14 Hours 21 Min 0 Sec	Generator	GENERATOR RESTART	Eke	BTS
Closed	TT0000000096606	South East	01-OBIARUKU	RSL link Failed		Cascade Site	Radiator Problem Resolved	Iyobosa Adanene.	BTS
Closed	TT0000000096607	North West	BOD001	LAPD_OML failure		Generator	GENERATOR RESTART	David Ogunsola	BTS
Closed	TT0000000096608			RSL link Failed		Cascade Site	Radiator Problem Resolved	Iyobosa Adanene, Samuel	BTS
Closed	TT0000000096613	Lagos	016_IKOSI_KETU	IT POWER TRIPPED VS	1 Day 7 Hours 32 Min 0 Sec	Generator	GENERATOR RESTART	Bola	BTS
Closed	TT0000000096614	Lagos	909_OKOKO	GENERATOR FAULT		Equipment	Reset System	Ibrahim	BTS
Closed	TT0000000096615	Lagos	459_ISHIASHI	GENERATOR FAULT		Equipment	Reset System	Ibrahim	BTS
Closed	TT0000000096617	Lagos	046_IDIMU	HIGH TEMP		Equipment	Reset System	Shola	BTS
Closed	TT0000000096620	Lagos	125_GUNKOYA_IKD	HIGH TEMP		Equipment	Reset System	Daniel	BTS
Closed	TT0000000096621	Lagos	478_IBONWON_EPE	HIGH TEMP		Equipment	Reset System	Daniel	BTS
Closed	TT0000000096622	Lagos	480_ITOIKIN_EPE	HIGH TEMP		Equipment	Reset System	Daniel	BTS
Closed	TT0000000096623	Lagos	206_SHOGUNLE	IT POWER TRIPPED VS		Equipment	Reset System	Ajiboye Shina	BTS
Closed	TT0000000096624	Lagos	058_MAGODO	HIGH TEMP		Equipment	Reset System	Seun	BTS
Closed	TT0000000096626	Lagos	945_OJUELEGBA	GENERATOR FAULT		Generator	GENERATOR RESTART	Obasi	BTS
Closed	TT0000000096627	Lagos	137_EXQ_PLAZA	CASCADE SITE		Generator	GENERATOR RESTART	Obasi	BTS
Closed	TT0000000096628	Lagos	620_ITIRE	GENERATOR FAULT		Equipment	Reset System	Obasi	BTS
Closed	TT0000000096629	South West	046_IITA	GENERATOR FAULT	0 Days 7 Hours 39 Min 0 Sec	Generator	GENERATOR RESTART	Kunle	BTS
Closed	TT0000000096630	South West	149_MONIYA	CASCADE SITE	0 Days 0 Hours 53 Min 0 Sec	Cascade Site	GENERATOR RESTART	Kunle	BTS

APPENDIX 2

(A) BSS DERIVED ERROR-LOG SUMMARY

Fault Type(Symptom) S	Root Cause C	frequency(No. of occurences	DURATION (IN HOURS)	*Alarm Codes*
LAPD_OML failure	Equipment Radio	861	14.84	***L****APDOF*
RSL link Failed	Transmission µW	1100	6.89	*RSLF*
Transmission Network Error	Transmission µW	46	8.4	***TxNetE***
BSS Internal Problems	Equipment Radio	82	27.3	***BSSIP***
VSWR fault	Transmission	1	15.2	***VSWRE***
Transmission rerouting	transmission Mux	6	11.52	***TxRR***
OAM Database not Found	Equipment server error	1	18.8	**OAMdBASE**

(B) MSC DERIVED ERROR-LOG SUMMARY

Fault Type(Symptom) S	Root Cause C	frequency(No. of occurences	DURATION IN HOURS	CODES
SIZE ALTERATION OF DATA FILES SIZE CHANGE REQUIRED	Equipment(OAM Dbase block low.	285	22.62	SIZALT
High Processor Load and Call limiting	Equipment (	2813	7.06	HPLCL
High processor load	Equipment(switching tx.)	106	3.69	HPL
Cannot monitor node	Equipment(System hanging	282		CMN
100% C7 link failure	Equipment Congestion	900	12.1	100%C7LF
CP FAULT	Equipment hanging	137	17.3	CPF
Call limiting	Switching equipment	78	2.1	CL
50% C7 link Interfailing	Transmission network problem	36	6	50%C7LI
EXCHANGE INPUT LOAD SUPERVISION	Equipment congestion)	398	8.98	EXINLS
FILE PROCESS UTILITY AUTOMATIC FILE TRANSFER FAILURE	Equipment(FTP Fault)	64	8.65	FPUAF
RP FAULT	Equipment (Processor fault)	247	15.96	RPF
CP- AP COMMUNICATION FAULT	Equipment (processor fault)	54	24.42	CP-APF
CCITT7 LINK FAILURE	Equipment (switcing Tx)	222	6.28	CCLF
GROUP SWITCH FAULT	Equipment (switching)	63	26.14	GPSWF
C7 Link interfailling.	Transmission (RSL level low)	15	1.24	CCLI
SOFTWARE ERROR	Software application/protocol stack err	11	34.12	SWERR
Charging destination fault	Equipment (charging proxy modem port) error)	19	10.67	CDF
Command log blocked	Equipment (configuration)	18	4.05	CLOGB
IPN Fault	Equipment (IPN/cp malfunction)	5	1.77	IPNF
CP state not normal	Equipment (dumping)	8	62.33	CPSNTN
DEVICES IDLE	Equipment hanging	10	0.95	DEVI
100% devices blocked	Equipment	41	35.07	100%DEVB
OMC not Responding	Equipment config, tx, &sw errors	209	1.82	OMCNTR
Faulty E1	Transmission (fibre)	3	78.52	FE1
Not processing calls	Equipment Rp error	12	4.16	NTPRC
NMC is unable to monitor	Equipment (OSS P/w error)	107	5.5	NUTMON

APPENDIX 3

(A) Conditional Probability Table of BSS Alarm summary

The parent set of is (BSS) =2096, and $C_k = 0.5$

Fault Type(Symptom) S	**Root Cause C**	**Frequency(No. of occurences** ( )	**Marginal probability** $\frac{(}{)} = Si, j$	**Conditional Probability Of S given C** $P(S_i=S_{i,j} / C=C_k)$
LAPD_OML failure	Equipment Radio	861	0.4106	0.8212
RSL link Failed	Transmission µW	1100	0.5248	0.8747
Transmission Network Error	Transmission µW	46	0.0295	0.0489
BSS Internal Problems	Equipment Radio	82	0.0391	0.0782
VSWR fault	Transmission	1	0.0005	0.001
Transmission rerouting	transmission Mux	6	0.0029	0.0057
OAM Database not Found	Equipment server error	1	0.0005	0.001

(B) Conditional Probability Table of MSC Alarm summary

The parent set of is (MSC) =6143, and C_k = 0.5

Fault yTpe(Symptom) S	**Root Cause C**	**frequency(No. of occurences ( )**	**Marginal probability (/)**	**Conditional Probability Of S given C** $P(S_i=S_{i,j} / C=C_k)$
SIZE ALTERATION OF DATA FILES SIZE CHANGE REQUIRED	Equipment(OAM Dbase block low.	285	0.0464	0.093
High Processor Load and Call limiting	Equipment (	2813	0.4579	0.9158
High processor load	Equipment(switching tx.)	106	0.0173	0.0345
Cannot monitor node	Equipment(System hanging	282	0.0459	0.0918
100% C7 link failure	Equipment Congestion	900	0.1465	0.2930
CP FAULT	Equipment hanging	137	0.0.0223	0.0446
Call limiting	Switching equipment	78	0.0127	0.0254
50% C7 link Interfailing	Transmission network problem	36	0.0059	0.0117
EXCHANGE INPUT LOAD SUPERVISION	Equipment congestion)	398	0.0648	0.1296
FILE PROCESS UTILITY AUTOMATIC FILE TRANSFER FAILURE	Equipment(FTP Fault)	64	0.0104	0.0208
RP FAULT	Equipment (Processor fault)	247	0.0402	0.0804
CP- AP COMMUNICATION FAULT	Equipment (processor fault)	54	0.0088	0.0176
CCITT7 LINK FAILURE	Equipment (switcing Tx)	222	0.03614	0.0723
GROUP SWITCH FAULT	Equipment (switching)	63	0.0103	0.0205
C7 Link interfailling.	Transmission (RSL level low)	15	0.0024	0.0049
SOFTWARE ERROR	Software application/protocol stack err	11	0.00179	0.00358
Charging destination fault	Equipment (charging proxy modem port) error)	19	0.0031	0.0062
Command log blocked	Equipment (configuration)	18	0.0029	0.0059
IPN Fault	Equipment (IPN/cp malfunction)	5	0.0008	0.0016
CP state not normal	Equipment (dumping)	8	0.0013	0.0026
DEVICES IDLE	Equipment hanging	10	0.0016	0.0033
100% devices blocked	Equipment	41	0.0067	0.0134
OMC not Responding	Equipment config, tx, &sw errors	209	0.034	0.068
Faulty E1	Transmission (fibre)	3	0.0005	0.001
Not processing calls	Equipment Rp error	12	0.002	0.0039
NMC is unable to monitor	Equipment (OSS P/w error)	107	0.0174	0.0348