A TMN Framework for Faults Diagnostic in Wireless Telecommunication Networks

M. Guiagoussou, R. Boutaba

Telecommunication and Distributed Systems Division
Computer science Research Institute of Montreal
1801 Avenue McGill College, Suite 800
Montreal (Qc) H3A 2N4 CANADA

Abstract

The occurrence of a fault in a critical component of large telecommunication system may cause multiple abnormal situations leading to large number of different alarms at different locations. Appropriate management tools are required to automatically filter and correlate these alarms in order to localize faulty components. Such tools must be based not only on the description, state and behavior of the managed components, but also on explicit description of the dynamic state and behavior of the relationships between these components. The paper explores the usage of relations between wireless network managed components within a TMN based framework. The proposed framework is used in the design of a TMN based fault management system including alarms correlation and fault diagnostic for wireless networks.

Introduction

A fault occurrence at the level of a critical component in large telecommunication systems may lead to several abnormal situations that may be observed at different locations and at different levels. The fault may be propagated and affect different services at the level of the whole distributed system. This often leads to the generation of a large number of alarms of different types and different formats received at different locations. Appropriate management tools are required to automatically : collect the alarms and user complains; filter and correlate them; identify the information relevant to the fault diagnosis and localization; isolate the faulty component and restore the system to its operational state. The tools must be based not only on the description, state and behavior of the managed components, but also on explicit description of the state and behavior of the relationships between these components. These relationships, are helpful for a better understanding of the overall system abnormal behavior. This is particularly important as current wireless telecommunication networks may involve very complex interactions at different levels and in different ways between a large number and variety of interconnected components. Specific issues such as the air interface or mobility management present new challenges to the telecommunication networks management community. Even if there are ongoing standards works for the management of GSM networks ([7], [8], [10], [11], [22]), still few works have been achieved in this specific area of wireless network management ([3], [4], [6], [5]). Hopefully, most of existing network management works addressing issues such as alarm filtering and correlation techniques, artificial intelligent fault diagnostic solutions for telecommunication networks can be reused for the specific needs of wireless network management ([19], [13], [24]). Based on previous achievements, we have further explored the use of relations as a support for an integrated management of wireless networks.

In this paper, we present a TMN framework and emphasis the utilization of relations between managed resources for fault management, mainly in alarm correlation and fault localization. Section 2 introduces the proposed management framework. Section 3 describes the information model and it's application to wireless networks. Section 4 describes a functional architecture for wireless networks faults management. Section 5 presents a design architecture. Section 6 summarizes the paper and presents ongoing works.

0-8186-7852-6/97 $10.00

1. A TMN-based Management Framework

The management framework proposed for wireless telecommunication networks fault management is mainly based on TMN concepts ([15]) such as the three TMN architectures (informational, functional, and physical architecture) and the TMN Logical Layers. We have used a hierarchical domain based organization of the management environment to describe the structure of the managed and management system [2].

The complexity of large scale wireless telecommunication networks management is reduced by structuring the management system into management subsystems and by distributing management responsibilities over these subsystems. A management by delegation mechanism ([31]) provides the overall management task. M.3010 [16] defines a breakdown of a Telecommunication Management Networks (TMN) into three architectural aspects : information architecture, functional architecture, and physical architecture. The Informational Architecture, describes the information that are exchanged between the physical blocks. It provides rational for the application of OSI systems management principles to TMN principles. The Functional Architecture, describes the appropriate distribution of functionality within the TMN to allow for the creation of functions blocks from which a TMN of any complexity can be implemented. Finally, the Physical Architecture, describes realizable interfaces and examples of physical components that can make up a TMN. The Logical Layer Architecture (LLA) is used for the layering of fault management Operation Systems Functionality. LLA is a development concept that is based upon hierarchical principles in which the architecture can be thought as being based on a series of layers. Five layers have been defined within ITU-T management framework [15, 17]: Business Management Layer (BML), Service Management Layer (SML), Network Management Layer (MNL), Element Management Layer (EML), and Network Element Management Layer (NEL). The scope of each layer is broader than the layer below it. In general, it is expected that upper layers will be more generic in functionality while lower layers are more specific.

2. Management Information Architecture

2.1 Generic resources and relations

Large telecommunication networks are composed of number of components interacting at different levels (e.g., communication, processing, storage, etc.) and in different ways (e.g., containment, interconnection, client/server, etc.) to provide the global telecommunication. A reliable and efficient provision of these services with the expected quality of service often lies on a good maintenance of the relations between the system components. However, these relations and dependencies between components may be themselves complex, not explicit, and hidden [13]. They are often described by uncertain and incomplete data. An explicit and accurate description of these relations and their dynamic evolution is very useful for example to optimize the localization of faulty components.

2.1.1 Basic Relations

We identified two generic categories of relations within telecommunication networks and distributed systems in general: ***structural relations*** (such as *aggregation* relation and *connectivity* relation), and ***cooperation relation*** (such as *use-of-service* relation). Relations are considered *basic* (e.g., *basic aggregation relation, basic connectivity relation* and *basic use-of-service relation*) when they are *direct* (i.e., with no intermediate interaction between managed components). Basic relations are then used as *building block* to construct more sophisticated and complex relations.

A basic aggregation is a relation between a composite object and it's immediate components. The role of a component in a composite object (e.g., critical resource of a multiplexing system such as power supply or processing unit) determines the dependency degree between the composite object and its components and thus the importance of the corresponding aggregation relation for the management processes. The components of an aggregation on which relies the existence of the composite object are called *dominant objects*.

A basic connectivity relation specifies a logical or physical connection between two communicating objects. Communication links are physical or logical network elements. Connectivity relation can either have *active* (e.g., data being transferred) or *idle* (i.e., the communication is inactive) state. In the active state, objects involved in connectivity relation can play *sender role* (e.g., trail termination source point), a *receiver role* (e.g., trail termination sink point), or both a sender and a receiver role (e.g., trail termination point bi-directional) [18]. Both active and passive connectivity are useful for fault analysis.

Cooperation relations are created, activated, and terminated (normally, abnormally, aborted, etc.)

between network and distributed systems components. By their own initiative or guided by an external actor, the involved components adjust their behavior or share resources in order to realize common objectives (e.g., provide a higher level service to user). An example of cooperation relation is the producer/consumer relation which is a specific case of the general client/server relation defined here as *use-of-service* relation [21]. This relation is relevant to the diagnosis process analysis at the occurrence of a service disruption or when the quality of service is degrading.

2.1.2 Combination of relations

The basic relations presented previously may not individually describe complex interactions in networks and distributed systems. However, they can be combined to describe more sophisticated dependencies relations such as a sequence of interactions. For example circuits are end-to-end connection which involves the end systems and intermediate components. Under an abnormal condition (e.g., an intermediate component failure), several side-effect faults can be detected in both directions (i.e., upstream or downstream) at different locations, and at different levels. Basic relations are composed to form a partial transitive closure. For example, an indirect aggregation relation of length *n* is the composition of n direct aggregation relations. In such a composed aggregation relation, the composite component (e.g., higher speed transmission path such as DS3) contains at least one intermediate component that, in turn, contains one or several other components (e.g., T1, E1). An indirect aggregation relation corresponds to a branch of the managed system hierarchy. Relations are sets of related managed components couples (e.g., binary relations). Thus, set operation "union" and "intersection" operators are applied to two or more types of relations in order to explicitly describe complex relations. Union operation defines alternative relations, while intersections defines simultaneous relations.

2.2 Wireless Network Informational Architecture

A generic architecture of a PLMN (Public Land Mobile Network) contains mainly the following components [1, 28, 29, 27]: Mobile services Switching Center (MSC), Home Location Register (HLR), Base Station Subsystem (BSS) composed of Base Station Transceiver (BST) and Base Station Controller (BSC), and Mobile Stations (MS) as illustrated by part of Figure 1. These components interact via wired connections and air interfaces [12].

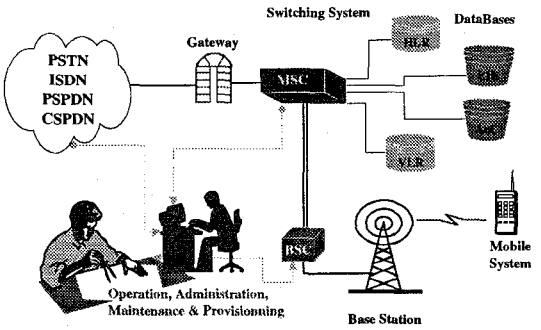

Figure 1 - Cellular networks Generic Architecture

2.2.1 Wireless Network Components Description

MSC/VLR: The VLR is the database that contains the information about visiting MS belonging to a foreign area. In practice, the VLR is integrated within the MSC. Therefore, the MSC and the VLR are referred as the composed entity: MSC/VLR. MSC is the central coordinating element that contains the VLR. Following are some of MSC main functions: transmission of signaling and speech between BS and MSC; collection and analysis of signal strength measurements, switching of calls to the appropriate BS; interrogation of routing data toward HLR and MSC-Home; updating the MS location information; maintenance of speech path continuity as subscribers move between BSs and between Services Areas. MSC is a telephone exchange which performs mainly call control and switching functions for Mobile Station within its geographical area.

GMSC: The gateway allows the mobile network to interface to the PSTN (Public Switched Telephone Network) and to other networks (fixed and mobile: ISDN, PLMN, etc.). The gateway is used for all calls from and to the PLMN and interacts with HLR to obtain information on the MS's current location.

HLR: Home Location Register (HLR) is a stand alone component of the mobile network. It is mainly composed of a data base that is in charge of data management of the registered Mobile Stations. It contains information about the Mobile Station (including foreign), moving around within the MSC area. Among other information, all subscription data and the current location of the Mobile Station are stored.

Base Station System: The base Station System (BSS) is in charge of the communication and controlling of the Mobile Station. Two main components are involved in the DSS : the Base Stations (BS) and the Base Station Controller (BSC). A *Base station* is responsible for a number of small areas called cells. This bloc handles the radio traffic within each

and received information about the components states and also the results of tests analysis.

3.1.2 Diagnosis OSF

Based on results of the alarm correlation process, a fault diagnosis is made within a given domain. A component is declared potentially faulty (highly suspicious) when a fault pattern involving this component is effectively identified from the processed alarms. This can be achieved locally (in a centralized manner) or distributed over cooperating fault managers. If the faulty component is not accurately identified, appropriate test sequences are repeatedly selected and performed on the remaining highly suspicious components. Test results and performance measurements [9] are analyzed so as to locate the exact set of faulty components. When many levels of the overall hierarchy are concerned with the detected fault, the diagnosis process may involve all these levels. A top down approach is used to refine the fault management process within a given domain by delegating the fault localization responsibility to lower-level domains, those that more likely contain the faulty component. This delegation can be applied recursively through many levels of the domains hierarchy with less suspicious components at each level and by executing more specialized test sequences. Each domain manager reports to its superiors the results of its diagnosis. The top down approach is often suitable when the fault is detected at a relatively high level (e.g., the service level). When a fault is detected at the level of a given domain, a bottom up approach is used to notify concerned higher-level domains and possibly the diagnosis result corresponding to this fault. This can be useful to prevent fault propagation and to set up the isolation/repair procedures. In addition to the hierarchical diagnosis, a peer-to-peer cooperation between managers of the same hierarchical level may be required to provide a consistent diagnosis.

3.2 Wireless Networks Fault Management Functional Architecture

Based on a domain decomposition and a logical layering, a functional architecture for the fault management of wireless networks is proposed. As illustrated in Figure 2 the correlation and diagnosis OSFs defined in previous sections are specialized for wireless networks at each of the five TMN logical layer, i.e. Business Management Layer (BML), Service Management Layer (SML), Network Management Layer (NML), Element Management Layer (EML), and Network Element Layer (NEL).

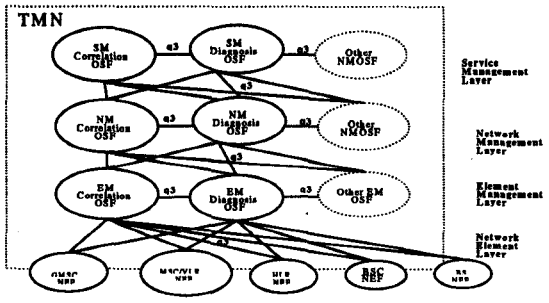

Figure 2 - Wireless Network Fault Management Functional Architecture

Fault management activities specific to a given layer are allocated to an OSFs of that layer. For example in the NEL, the correlation OSF blocks functionality is related to the collection and analysis of monitoring information within and around the wireless network elements. This OSF is capable of correlating alarms related to multiple devices of an individual NE. The diagnosis OSF block functionality is related for example to diagnostic testing activities or a higher level of correlation. Similarly, the EML OSFs performs correlation and diagnostic functions within a set of NEs in either local or remote operations. At the Network Management Layer, the operational states of end-to-end circuits together with all information on interconnection relations health state are provided for fault management purposes. SML, interacts with the customers for fault management service matters based on well established enterprise building blocks for the delivery and management of these services.

At the service boundaries of the fault management OSF blocks, q (q3 or qx) reference points are defined as access to the services [17]. They represent conceptual points of information exchange between these blocks. For example, they identify information that passes between correlation OSF and diagnosis OSF. These information include mainly: the list of correlated alarms that are used by the diagnosis OSF to accurately identify fault patterns, and the list of highly suspicious managed objects. The diagnosis OSF could also generate alarms informing the correlation OSF that a component is recognized to be faulty. Another q reference point is defined between two OSFs located in two adjacent layers (e.g., Service Management OSF and Network Management Layer OSF).

4. Faults Diagnostic System Design Architecture

In order to deal with complex faults, it is necessary to have, on one hand, an accurate knowledge about the

cell (from and to a MS). The *Base Station Controller (BSC)* is part of the whole Base Station system Network Element level. It administers the radio network, i.e. the cells and their radio channels, by continually collecting statistics on the number of calls, successful or unsuccessful handovers, traffic per cell, etc.

2.2.2 Relations between wireless network components

Relations between the mobile cellular network components at all level (i.e., service, network, network element, networks element subsystems or software blocks) are relevant for the faults management process. They provide a basis for the fault pattern and propagation recognition. They are also useful when correlating alarms. They can be used to guide further diagnostic testing and measurements activities. Results analysis and fault localization can also be based on the information collected on the interactions between physical network components and the signal exchanged between software elements. Only aggregation relation and inheritance relations between generic classes have been presented in previous sections. From the network fault management perspective, the following two other relations must be considered : the *connectivity* relation and the *use of service* relation.

From the user perspective this relation ties a customer or an user to a given mobile service provisioning point or a managed element service access interface. From the managed element perspective, the use-of-service relation is defined either between two or several equipment/software within a managed element or within different managed elements, or between a software and an equipment within a managed element. Several instances of use-of-service relation class can be identified at a functional level during a call provisioning (e.g., «call set-up», «voice channel allocation», «transmission control», etc.) and used during the fault analysis.

3. Functional Architecture

This section focus on fault management Operation System Functions (OSFs). In the scope of wireless networks management, a domain manager may be either dedicated to the fault management task (a fault management domain) or performs fault management together with other management functions (e.g., configuration, performance, etc.). The manager supervises and controls resources in a fault management perspective reacting and/or preventing fault occurrence [30]. Only fault management OSF blocks will be detailed in this paper.

3.1 Fault management OSFs

Faults management is one of the five basic network management area defined within ISO management [14]. It can be decomposed into four OSF: Monitoring, alarm analysis, fault localization and fault recovery. Monitoring OSF is needed for all management activities including performance management, configuration management and fault management. It is an essential means for obtaining the information required about network and systems components. The behavior of the system is observed (event detection) and monitoring information is gathered and disseminated (notifications) [23]. In the scope of fault management, monitoring information are alarms generated by the managed resources and/or sent by the monitoring agent to notify the occurrence of faults. The processing of these alarms consists mainly in discarding superfluous and non relevant event notifications. Alarm analysis OSF can be decomposed into two main activities: filtering and correlation. Alarm filtering discards lower priority alarms or stores them in a log file ([19], [24]). Correlation recognizes commonalties between alarms and discards non significant ones and side-effects [21], [26]. Fault diagnosis OSF consists to perform deeper analysis of appropriate tests result in order to locate the fault origin by reducing the suspicious components to a limited set containing optimally a single component that is the faulty one ([3]). Fault recovery OSF consists to restore the system to its normal operation either by isolating the faulty component or by repairing it. In the following, we will focus on alarm analysis and fault diagnosis OSFs.

3.1.1 Alarms Correlation OSF

Alarm correlation consists to detect commonalties between alarms, determine the principal alarms and discard their side-effects (e.g. redundant alarms). It varies from simple messages filtering and redundant alarms suppression to more sophisticated alarms compression and generalization/specialization. The correlation process also allows to reduce the number of suspicious components thus reducing the work of diagnosis process. The fault localization process can then be based on the remaining non redundant alarms. The correlation process is iteratively executed by updating a set of potential faults and a set of suspicious components according to the newly received alarms

dependencies between the components [21], [20], [13] of the managed system, and on the other hand a support which allows the components of the managing system to cooperate for the establishment of harmonized, non-conflicting and efficient diagnosis.

4.1 Relations-based Alarms Correlation

A correlation is the statement of similarities between alarms generated by managed components ([24], [26], [25]). It attempts to reduce a given set of alarms to a smaller subset. Several correlation procedures have been defined in previous works [19], however the conditions in which these procedures are to be used were not clearly defined. In the following we describe some correlation procedures as well as samples of their utilization rules. We then present a generic correlation policy and directions toward faults diagnostic solutions based on relations between the management components.

4.1.1 Correlation Operations

An alarm notification reports several information about a fault-related event including the identification of concerned component (i.e., notification sender and/or suspicious component), the description of the observed abnormal conditions, the event occurrence time and the possible causes of the detected fault. Correlation operations acts on these alarms in order to reduce their number. Well known operations are [20, 21]: suppression, substitution, compression, generalization, and specialization. *Suppression* consists to discard (or store in a log file) alarms that satisfy specified conditions (e.g., alarms of a given type or alarms that have a property that fall outside a legitimate interval). *Substitution* aims to replace a specific set of correlated alarms by a new one. *Compression*, *generalization*, and *specialization* are specific cases of substitution. Compression reduces several equivalent or identical alarm to a single alarm. It is useful for processing alarm streams (multiple alarms generated by the same faulty components). Generalization replaces an alarm by an instance of its super-class. This allows to substitute a set of low level (e.g., Network Element Management Layer) alarms by a more abstract high level one (e.g., Service Management Layer). Specialization allows to substitute an alarm by a more specific one, i.e. an instance of one of its subclasses.

4.1.2 Utilization Rules

The goal here is to define the conditions that must be satisfied in order to activate the correlation process (i.e., execution of appropriate correlation procedures). These conditions reflect the occurrence of situations such as the recognition of alarm patterns [25], [24], or the detection of a given fault scenario. The conditions we would like to highlight in this paper are those related to relations we have defined previously. For example, priority characterizes the importance of a component on alarms from a fault management perspective. It can be used for alarms filtering, i.e., suppressing or logging of low priority alarms. There are several criteria to be used for the allocation of priorities. Time stamps in alarms is used for example to discard all alarms that are not significant from a time perspective (i.e., time expired [20]). In general, the main criteria for priority allocation is the level of service degradation caused by the reported problem. A way to estimate the potential impact of a fault is to use the dominance characteristics of composite objects within an aggregation. In a cellular switching system for example if a problem occurs within an MSC software or hardware block (i.e., dominant component of the switching system), high priority is assigned to the alarms stemming from this problem because all the switching services will be potentially affected. Relations and priorities are used to define conditions necessary for the activation of correlation procedures introduced so far (suppression, substitution, generalization, specialization). Most of these correlation operations use basic suppression operation. The later will be emphasized through the following illustrative cases. Consider that two communicating managed objects: an MSC and a PLM Local exchange (LE) are interconnected via an intermediate failing object (say the GMSC). In this case, the two end point objects, the MSC and the LE will experience difficulties and possibly send alarms. In addition, if an alarm on the intermediate failing GMSC have been received, the two end connection objects alarms could be side effects of the GMSC failure. The two end alarms are then assigned lower priority and suppressed or logged.

This way the satisfaction of predefined correlation conditions trigger the execution of one or several correlation operations which allow to suppress irrelevant and low priority alarms or store them for future analysis. The correlation procedures defined above are executed whenever the corresponding conditions are satisfied. Direct and indirect relations and their combinations are used to define these conditions that describes the activation rules.

4.1.3 Alarms Correlation Policy

A network configuration contains a description of its components together with the relationships between

them (mainly communication links). We have enriched such configuration by introducing the usage of relations description and defined the following higher level correlation policy that is described in terms of the following steps (not necessarily sequential):

1. Actual relevant information on managed object states, behavior and relations are obtained by accessing the management information base or requesting the configuration manager to provide any dynamic change that can affect the fault management process.
2. Strategic combinations of relations (composition, intersection, and union) are explored and calculated if necessary. Information on intermediate objects, together with basic relations are computed or loaded for the purpose of the analysis process.
3. Correlation conditions are checked and, according to the appropriate rules, correlation operations are selected and executed upon the received alarms which verify the correlation conditions.
4. According to the alarm correlation resulting from the third point, innocent suspicious components are removed from suspicious components' list and a list of faults pattern are updated. The latter is particularly important for limiting the number of faults causally related (side effects) and determining the highly suspicious component to be processed by the fault diagnosis phase.

4.1.4 Fault Diagnosis Issues

Depending on the type and priority of remaining faults in the set of non resolved faults that results from the correlation process, one or a combination of the following diagnosis strategies can be applied on the list of highly suspicious component resulting from alarms processing :

- *Service based analysis* : consist to investigate faults by analyzing networks and distributed systems behaviors from the level (e.g., quality) of service disruptions perspective. This includes all cooperating managed components involved in the provisioning of affected services source clients and targeted servers, as well as all intermediates entities involved in all service provisioning transactions (SML, NML, EML, NEL)
- *Connectivity based analysis* : consists to analyze all components and interactions signals (e.g., bit errors rates) in the suspicious path from a connectivity perspective (path analysis) [13]. This direction is useful after a combined relation have been identified to be highly suspicious. An investigation of the connectivity path could help locate the faults that affect service provisioning at a lower level (NML, EML)
- *Aggregation based analysis* : consists to analyze aggregation relations in a top-down or a bottom-up approach (tree search approach in [13]). This can be achieved according to the fault nature and the position of the suspicious component in the aggregation relation tree. It's meant that the analysis of all aggregation relation instances from the highest level composite object to the lowest level objects (i.e., at the leaves of the aggregation tree) or the other way around.
- *Diagnostic Testing:* In each of the previous alternatives, if the results of correlation operations, service, connectivity, and aggregation relation based analysis, or further logged alarms analysis don't lead to a conclusive diagnosis, appropriate diagnostic tests must be performed on the remaining highly suspicious components and their relationships. Automated and intelligent selection, execution, and interpretation of results of tests sequences remains the ultimate strategy to be used.

4.2 Fault Management System Design

The initial sources of fault management information are mainly the monitoring agents, the network service users and possibly other functional areas such as configuration management. The flow of management information on both directions (bottom up and top down) between lower management layer and higher management layer (bottom up) is depicted in Figure 3.

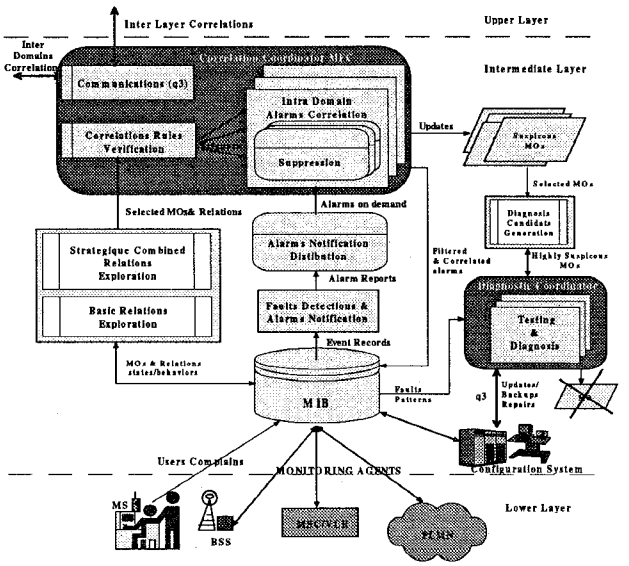

Figure 3 - Alarms Correlation Architecture based on Relation

A Management Information Base is designed to maintain the logical representation of real resources (MOs), their interactions, and additional support objects (SOs) that are useful for the fault management matters (e.g., networks events records, alarms log, alarms statistics, historical data, fault patterns, correlation rules, diagnostic tests, etc.). Implicit, but complex relation are computed from the basic relations and stored as managed object for use by the correlation and diagnosis processes (e.g., while checking the correlation rules or selecting diagnostic tests). The management view (MO/SO, OSF, reference points, etc.) of the domain structuring and the logical layer decomposition are also maintained within the MIB. Correlation procedure is either conducted by a local manager (OSFs) within a given domain or in cooperation with manager from other domain or from different layer. The local process consists mainly to explore basic relations and select those that can be combined form complex but strategic one. Based on the collected alarms and if available, knowledge of the diagnosed fault (e.g., alarms pattern, known fault scenario), those relations that are relevant for the fault analysis are computed. Then correlation rules are checked. When the correlation rules are verified, the execution of correlation operations (e.g., compression, suppression) are trigger. As the alarms are correlated, innocent components are discarded, and suspicious components can be more accurately identified, and proposed to the diagnosis process as candidate for further diagnosis. Tests and deeper analysis are then conducted on these candidates and the faulty component is isolated based on the diagnostic tests results analysis.

4.3 Implementation status

The implementation of the proposed design is undergoing. Our platform is CORBA compliant (ORBIX) and supports the development of fault management OSs. Correlation and Diagnostic routine based on relations between components have already been implemented. A management information base (MIB) containing the generic cellular switching system (i.e., it's components and their basic/composed relations) representation have also been specified and compiled in GDMO. A pseudo Q3 interface between the OSs and the MIB agent have been also implemented as CMIS/IDL interfaces. In the near future, we are planning to built a testbed for the achievement of the whole cellular network fault management system.

5. Summary

In order to deal with more types of faults that can occur in large networks and complex distributed systems such as wireless networks, we have introduced a TMN based fault management framework enhanced by the use of relations between the managed system components as a support for alarm correlation and faults diagnosis. Although several aspects related to fault management have been discussed, the ultimate aim of this paper is to show how much a precise knowledge and an up-to-date maintenance of relations can be useful in the correlation process and the diagnosis decision. The advantage of the proposed approach is its ability to address complex situations by decomposing any encountered problem into sub-problems following the management system hierarchical structure. It is based mainly on a recursive refinement versus abstraction of the alarm correlation and fault diagnosis results through different levels of the hierarchy while taking into account the collected information not only on the managed components but also on the relations between them. The paper has also pointed out several issues requiring further developments to achieve efficient and automated support for fault management.

6. References

[1] Bijan Jabbari et Al., *Network Issues for Wireless Communications*, IEEE Communications Magazine, p. 88-98, January 1995.

[2] Raouf Boutaba, Simon Znaty. *An Architectural Approach for Integrated Networks and Systems Management*, in ACM-SIGCOM Computer Communication Review, ACM Press, Vol. 25 Number 5, page 13-39, October 1995.

[3] S. Brugnoni et al., *An Expert System for Real-time Fault Diagnosis Integrated Network Management*, San Francisco, Californie, pages 617-628, 1993.

[4] Bugsch, A.; Schroter, M., *Network management for a public land mobile network*, IEE Colloquium on 'Network Management for Personal and Mobile Telecommunications Systems', p. 5/1-14, 1994.

[5] Chee-Meng Low, You-Tong Tan, Soo-Yong Choo, Sie-Hung Lau, Soo-Meng Tay, *AutoCell-An Intelligent Cellular Mobile Network Management*, IAAI-95, 1995.

[6] *S., Chia, Network Operational Principles for Third-Generation Mobile Systems*, British Telecommunications Engineering, 1993.

[7] GSM 12.00*: Objectives and structure of GSM PLMN management*, 1994.

[8] GSM 12.01*:Common Aspects of PLMN Management*, 1994.

[9] GSM 12.04: *Performance Management and Measurement for a GSM*, 1994.

[10] GSM 12.11: *Fault Management of Base Station System*, v1.3 1994.

[11] GSM 12.20: *BSS Management Information*, 1994.

[12] GSM 12.21: *Network Management procedures and messages on the A-bis interface*, 1994.

[13] K. Houck, S. Calo, A. Finkel, *Toward a Practical Alarm Correlation System*, Integrated Network Management IV, page 227-237, IFIP 1995.

[14] ISO/IEC 7498-4, Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 4 : *Management Framework*, 1989.

[15] ITU-T Recommendation M.3000, *Overview of TMN Recommendations*, Geneva 1994.

[16] ITU-T Recommendation M.3010, *Principles for a Telecommunications Management Network*, Geneva 1992.

[17] CCITT 3020 : TMN Interface Specification Methodology, 1992.

[18] ITU-T Recommendation M.3100, *Generic Network Information Model*, Geneva 1995.

[19] Gabriel Jakobson, Mark D. Weissman, *Alarm Correlation*, IEEE Network, pp. 52-59, November 1993.

[20] G. Jakobson, M. Weissman, *Real-time telecommunication network management: extending event correlation with temporal constrains*, Integrated Network Management IV, page 291-301, IFIP 1995.

[21] Jordan, J.F.; Paterok, M.E., *Event correlation in heterogeneous networks using the OSI management framework*, in Proc. of the Int. Symp. on Integrated Network Management III, H.-G. Hegering and Y. Yemini, eds., IFIP, CA, USA. Vol: C-12 pp. 683- 95, 1993.

[22] Lord R., Kelly J., *Challenges of specifying and implementing Q3 interface network management interface in a GSM network*, IEE Colloquium on Network Management for Personal and Mobile Telecommunication Systems, 1994.

[23] Masoud Mansouri-Samani, Morris Sloman, *Monitoning Distributed Systems*, IEEE Network, page 20-30, November 1993.

[24] M. Moller, S. Tretter, B. Fink, *Intelligent filering in network management systems*, Integrated Network Management IV, page 304-315, IFIP 1995.

[25] Y. A. Nygate, Event Correlation using Rule and Object Based Techniques, Integrated Network Management IV, page 279-289, IFIP 1995.26] B.M. Osborn, C. T. Whitney, *Object orientend correlation*, BT Technologie Journal, Vol 11, p. 131-142, 3 July 1993.

[26] B.M. Osborn, C. T. Whitney, *Object orientend correlation*, BT Technologie Journal, Vol 11, p. 131-142, 3 July 1993

[27] Jay E. Padgett, Critpopher G. Guther, Takeshi Hattori, *Overview of Wireless Personal Communications*, IEEE Communications Magazine, p. 28-41, January 1995.

[28] Raj Pandya, *Emerging Mobile and Personal Communication Systems*, IEEE Communication Magazine, p. 44-51, June 1995.

[29] J. Scourias, *Overview of Global System for Mobile Communication*, internal report, University of Waterloo, May, 1995.

[30] Thomas T. Towle, *TMN as Applied to the GSM Networks*, IEEE Communications.

[31] Y. Yemini et al., *Network Management by Delegation*, in Integrated Network Management II, I. Krishnan and W. Zimmer, Eds. North Holland, 1991, pp. 95-107.