A Recommender System Architecture for Network Management System

Sarath Kumar Reddy M[1] Jithendra Mungara[2]
[1]M.Tech Student [2]Professor & Dean PG Studies
[1,2]Department of ISE
[1,2]RVCE Bangalore, India

Abstract— Generally now a day's telecom networks generate massive a mounts of monitoring data consisting of observations on network faults, configuration, accounting, performance, and security. If there are any constraints/problems in the network the traditional reactive management approaches are increasingly stretched beyond their capabilities. By configuring, stabilizing, monitoring the live network will make the engineer's to react in a Speedy manner to the current changes. Following the new way for NMS where the problems can be easily identified and rectified.With this NMS both netwotk and services within the network are managed centrally so that the operator can view network elementfailures,servicequality indicators and traffic from one Screen.

Key words: Network Element (NE), Network Management System (NMS), Fault Management, Configuration Management, Performance Management, Security Vulnerability Monitoring (SVM)

I. INTRODUCTION

NMS is a new generation network management system for multivendor and multi-technology networks. NMS serves both as a network management system and as an element management system. NMS offers a wide range of unified operation and maintenance capabilities for network elements in core, radio and transport networks. It consists of many tools for handling a number of network elements and expanding networks. It is designed for handling an increase in both complexity of the network and the amount of traffic and data. Also, as heterogeneous networks are becoming a reality with the deployment of micro-, femto-, and picocells[1], the complexity of the operation and management (O&M) tasks [2] scales up accordingly. Following this growth of users and devices, by 2020 the total number of connected devices will reach up to 50 billion [1].

By introducing this concept, the entire network can be managed in single monitor which makes an easy way for us to identify the problems, to debug the NE issues and continuously monitoring.

The main cause to develop the NMS is to maintain faults on the monitor, performance of the network, configuring the network, providing the security to the network[4].

NMS provides the following management functions:

- Fault management
- Optimization
- Configuration management
- Performance management
- Security management
- NMS administration

The NMS system with management functions, applications

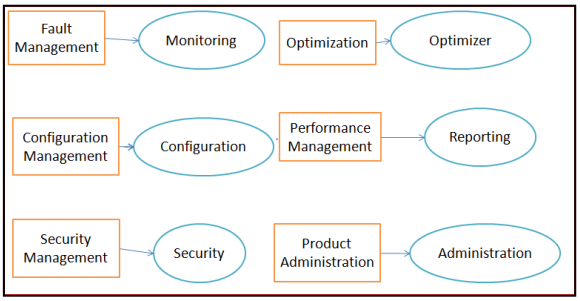

Fig. 1: Generalization of NMS & its Features

II. BACKGROUND

The combined effect of the increase in users and communicating devices, demand for service quality and diversity, support for mobility, and desire for social connectedness and communication has driven unprecedented and exponential growth in telecom network management data[3]. If the procedure of solving the problems is done manually ,it takes lot of time for finding in which NE it is having problem and it takes time for solving the issue in the NE. Going forward the population is increasing rapidly, connected devices also will get increased. The amount of data to be stored in the NE has to increase accordingly.

For example, Customers do more number of calls on Dec 31st, there is a need to increase a RAM size in each NE for that particular day. Manually doing is big challenge for telecom owners. After that particular day , there needs to be decrease RAM size so double extra work which is a big hurdle.

Many of the tasks required of human network managers are repetitive and involve wading through huge amounts of monitoring data. A new network management paradigm is required that is capable of automating the monitoring and repetitive tasks, and most importantly leverage massive volumes of network trace information to deploy a pre-emptive rather than reactive approach to predict issues and suggest timely appropriate remedial or preventative actions for network management.

III. FAULT MANAGEMENT

In NMS, fault management component provides the end-to-end solution for extraction, loading, filtering, and correlation of faults in real-time. The NMS system provides fault management functions with versatile monitoring tools integrated on top of the Monitor.

The alarm collection and processing engine provides the basis for fault management in the NetAct System. When an alarm occurs in the network, an alarm event is created. The alarm collection engine collects the alarm events and processes the events before storing them in the database.

Fault management events included in fault management processes are:

1) Alarm
2) Cancel
– Automatic cancel
– Manual cancel
3) Acknowledgement
4) Unacknowledgement
5) Change event
6) Alarm upload (synchronization)

The most common fault management actions are:

A. Manual and Automatic Alarm Cancellations:

An alarm cancel is a message that clears an alarm when the network overcomes the fault situation. To manage a network, it is important to indicate the end of an alarm situation. If alarms are not canceled, you cannot get accurate and up-to-date view of the network situation. To integrate into an operation and maintenance system, the alarms of all external systems must have a functionality to cancel the alarm automatically when the fault situation is complete. If the alarms do not contain automatic alarm cancellation functionality, manually cancel the alarms. Since manual cancellation is time consuming, automatic cancellation function must be implemented for all alarms.

B. Acknowledgement and Unacknowledgement Of Alarms

If an alarm is raised, acknowledge the error condition to indicate that appropriate corrective action will be taken.

C. Alarm Upload:

Upload the alarms from network elements database to NMS centralized database to ensure that the databases contain consistent alarm information. Alarm uploads in done:

1) After a network element is connected to NMS for the first time.
2) After the connection between NMS and the NE is broken, but was restored later.
3) On a regular basis at certain intervals.

D. Alarm Collection and Processing:

The alarm collection engine collects and pre-processes the alarms. The alarms with topology information are stored in the fault management database, and then forwarded to the alarm correlation engine, which performs the correlation rules. Depending on the selected filtering attributes, the alarms are loaded in the Monitoring Desktop applications at defined intervals.

Alarm collection engine provides enhanced alarm processing functions. It consists of scalable alarm pipes which collect alarms from various network elements.

E. Maintenance Mode:

This mode is used, for example, if the network element is currently under repair or maintenance. This stops NMS from processing alarms from that network element until the issue is resolved.

Monitor supports different control modes. When the maintenance mode is set, the network element reports under repair state and an alarm Object under maintenance is raised and displayed in the Alarm List and Alarm History tools.

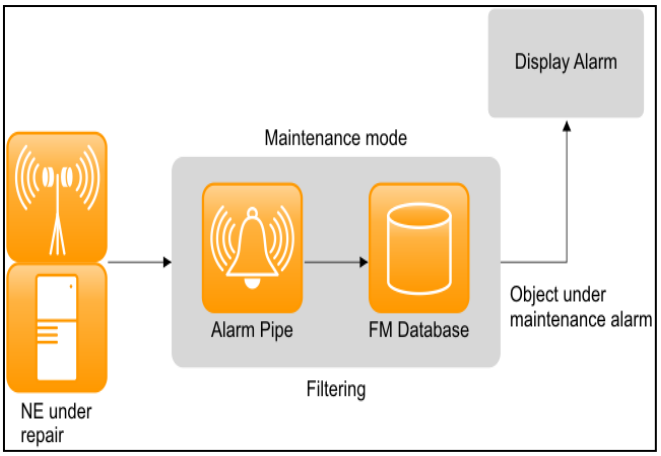

Fig. 2: Maintenance Mode

IV. Optimization

Optimization mainly takes place when the performance is under the line to be achieved or it comes when the behavior of new NE to be optimized. . In this phase, the relations between performance indicators and element parameters are analysed. After the analysis phase, the configuration parameter settings are optimized and the set quality criteria are checked. When the corrections are done for the NE the quality cycle starts from the start.

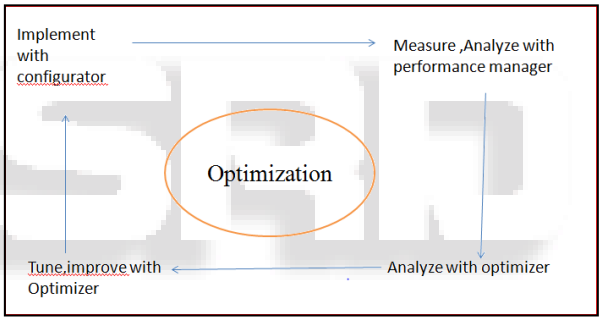

Fig. 3: Optimization Cycle

V. Configuration Management

Configuration Management is used for identifying and documenting the characteristics of network configuration data, viewing network data and provisioning changes and verifying compliance with specified requirements. With this, you can manage different network domains and network technologies such as GSM,LTE.

Configurator applications you can perform network-wide configuration management operations.Configurator provides one centralized data storage and the same tools and processes for all configuration management operations.

VI. Performance Management

The performance management applications that you can use for analysing and troubleshooting your network. Performance Manager is a family of applications for processing, analysing, and visualizing performance data that is coming from different sources. Raw data becomes meaningful information that is visualized in graphical and textual reports. Performance Manager gives a view of the network and service performance and makes it possible to

analyze network data, create reports based on the data and distribute the information within your organization.

Performance Manager is multi vendor-capable and collects data from your entire network that consists of NE and from other vendors. Performance Manager processes and stores the data, from days to years, depending on your requirements. Performance Manager includes also several ready-made report packages.

VII. SECURITY MANAGEMENT

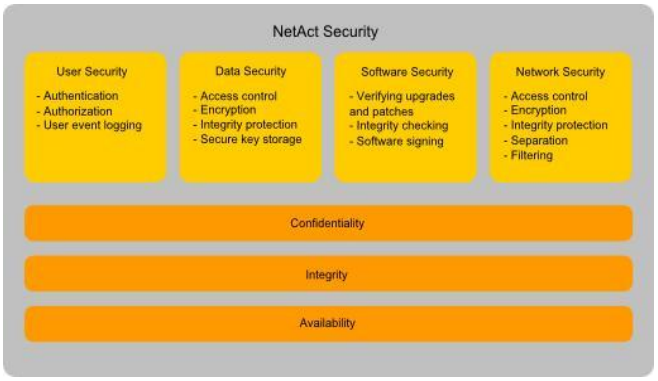

Fig. 4: Security Management

Security management consists of user security, data security, software security, and network security. Security management can be divided into the following areas which serve for all aspects of security management. These aspects are confidentiality, integrity, and availability. They are realized by user security, data security, software security, and network security.

A. System hardening:

System hardening is performed to prevent unauthorized internal and external use of the system. It covers user security, data security, software security, and network security.

B. User Security:

User security consists of authentication, authorization, and user event logging. Authentication is managed by the User Management application and authorization by the Permission Management application.

C. Network Security:

Connections to network elements are managed by the Network Element Access Control application.

D. Security Supervision:

Security supervision is performed through logging and tracing with the Monitor and Audit Trail applications.

E. Software Security:

Software security includes verifying software upgrade and patching processes, file integrity checking, and software signing.Software security in NMS means verifying that operating system and third-party software updates and patches as well as updating and patching processes, do not harm the operation of the system. The process of ensuring sufficient software security is referred to as Security Vulnerability Monitoring(SVM).

F. Network Security

Network security includes traffic access control, monitoring and protection including encryption, integrity protection, separation and filtering.

Network security in NMS means protecting the traffic in a network where NMS is used. The confidentiality of the traffic is ensured by using different encryption protocols.

VIII. NMS ADMINISTRATION

As a network management system designed to operate and maintain a complex telecommunications network, NMS needs to be up and running always.

In NMS, system reliability is ensured through the following basic features:

1) High availability in the hardware configuration, virtual infrastructure, and select software components to eliminate single points of failure in power, disk, memory, CPU, network connectivity, virtu-al machine, or service availability.
2) Load balancing, which takes care of the distribution of server load within a WebSphere Application Server cluster and the distribution of resources within the virtual infrastructure.
3) Online and offline backup and recovery solutions using v Sphere Data Protection and the NMS Backup Tool.
4) System Self-monitoring for internal fault and performance management.
5) Preventive Health Check, which is a tool that verifies the NMS System status.

IX. NMS VIRTUALIZED ARCHITECTURE

In a virtualized infrastructure (VI), software is set up in such a way that it can operate independently from the underlying hardware. The physical resources of multiple machines are shared across the whole infrastructure, and they act as a resource pool. In a VI, the physical hardware resources are divided into smaller units, virtual machines (VMs), that have their own allocated virtual CPU and memory.

The NMS virtualized infrastructure is based on the VMware solution. The following list summarizes the benefits of having a VI:

1) Hardware can be utilized more efficiently with the virtual machine granularity.
2) High availability is enhanced.
3) Scalability can be targeted more accurately.
4) Zero downtime during hardware maintenance is possible.
5) The virtualized infrastructure allows new ways of implementing disaster recovery.
6) NMS migration can be carried out without additional servers.
7) Downtime during software upgrade and migration is minimized.

X. SCALABILITY IN VIRTUALIZED INFRASTRUCTURE

Scalability is an important feature of the virtual NMS environment since there are software components that can be located on more than one VM, and conversely, one VM can contain more than one software component.

If the load increases beyond a virtual machine's ability to handle the load, then the software component and/or virtual machine must be scaled to cope with the increased demand. However, not all soft-ware components scale in a similar way

Some software components are designed to scale horizontally, which means that additional virtual machines need to be provisioned in order to enable the software component to distribute its load. Horizontal scalability's enabled by placing software components behind load balancers.

Other software components scale better vertically, which means that additional resources (CPU and memory) need to be allocated to the virtual machine where the software component is hosted.

XI. CONCLUSION

By automatically checking the consistency of your network parameters, typically numbering in millions, NMS helps you improve your network quality. NMS Monitor helps you find essential data quickly. It manages a huge number of alarms and identifies root causes across multiple network domains, technologies and vendors.

REFERENCES

[1] Ericsson, "More than 50 Billion Connected Devices," http://www.ericsson.com/res/docs/whitepapers/wp-50-billions.pdf; Ericsson Whitepaper: Feb. 2011.
[2] Infonetics Research, Subscriber Data Management Software and Services, 2nd ed., Nov. 2011.
[3] J. Keeney, S. van der Meer, and G. Hogan, "A Recommender-System for Telecommunicatons Network Management Actions," Proc. IFIP/IEEE. Symp. on Network Management 2013—TechSessions, Ghent, Belgium,2013, pp. 760–63.
[4] B. Jennings et al., "Toward Autonomic Management of Communications Networks," IEEE Commun. Mag., vol 45, no 10, 2007, pp. 112–21.

