An Overview of Network Management System

Ms. Priti V. Wadal
M.E. [2nd Sem, F.T] Computer Science & Engineering.
PRMIT & Research Badnera.
Pritiwadal7@gmail.com

Prof. Dr. S. R. Gupta
Computer Science & Engineering.
PRMIT & Reasearch Badnera.

***Abstract* — As the new services & users are increasingly added to the communication Network, so that management of such network become critical to provide assure quality of service. Finding skilled managers is often a problem. There is great change in demands of network management; any network management system is process of development & perfection.**
This paper explores one of the aspects of Network management system as telecommunication network management system & also the application of simple network management protocol to the management of network. Currently most network management system operates on SNMP. Then this paper explores potential uses of mobile agents in Network Management, Security in network management system and also review of current and other research activity in this area.

***Keywords*- Network management, mobile agents, Traditional Network management system architecture, telecommunication network management, security.**

I. INTRODUCTION

Network Management System refers to a utility or set of utilities designed to allow a network administrator to monitor and ensure the health of a network. A Network Management System will typically monitor both hardware and software components of a network. Network Management System utilities typically record data from remote points on a network for central reporting to administrator.

A network management system (NMS) is an automated system tool that helps networking personnel perform their functions efficiently [2].

The International Organization for Standardization (ISO) network management model defines five functional areas of network management.

The paper is organized as follows.

1. Network management functionality.
2. Traditional network management system architecture.
3. SNMP: One Critical Component to Network Management
4. Telecommunication network management system.
5. Mobile agents for network management.
6. Security in network management system.
7. Research activity.

II. BACKGROUND

In the past, the networks were too small. Moreover, it was easy to maintain the networks manually. Network size is increasing gradually with the increase of nodes in a network that is sub network. It is complex to maintain large networks like WAN. To overcome this problem, network management came in to existence. Network management is more than just managing networks. By the 1920s, AT&T had designed its network to meet the demands for quick, efficient service at the peak periods of a normal business day. But unusual events, such as holidays and natural disasters, could cause delays. Handling these events required active, coordinated management of the network as a whole.

III. NETWORK MANAGEMENT FUNCTIONS

ISO Network Management Model has five functional areas [1]

A. Fault management

Fault management (FM) comprises the following aspects [5, 6]

- Alarm surveillance-a monitoring aspect of the network management activity that looks into obtaining the information and processing to identify events of interest.
- Fault localization-a fault identification aspect of the fault management task.

B. Performance management

Performance management (PM) refers to ensuring that the network performance does not fall from the expected level. This task can be split into the following.

- Quality of services (QoS)-ensures that the offered QoS is achieved or an alarm is raised.
- Performance monitoring-similar to alarm surveillance as mentioned in the FM.
- Performance analysis-similar to the fault localization of FM.
- Performance management control-a control measure taken to bring the network back to normal behavior, meeting the assured quality of service.
- Traffic management-looks into the traffic management in the network and its behavior.

C. Configuration management

Configuration management (CM) comprises two parts.

- Collection of the monitoring information and display to appropriate centers in the required format.
- Network restoration in the case of node/link failures.

D. Security management

Security management (SM) can be viewed as having two aspects.

- Preventive approach-strengthens the existing security protocols.
- Reactive approach-assumes, in spite of having a strong protocol, that intrusions are still likely, catching them is the task here.

E. Accounting management

Accounting management (AM) is essential and is considered most important for the obvious reason that the whole service provided is not devoid of economy.

IV. TRADITIONAL NETWORK MANAGEMENT SYSTEM ARCHITECHURE

Network management system is a platform independent, portable, scalable, easy to configure and automatically maintains accurate and up to date client applications.

Components of NMS architecture provide interface between protocol specification and OSS applications like APP server, .net server application, implemented by their language code. Protocol implementation change depends on OSS requirements. GUI components will provide user interface to the user, easy to understand administration screens, fault browsers, mapping and performance chart views.

A network management component depends on network topology [9], nodes may increase or decreases in the network, network topology have to discover and update the nodes, which are coming into the network. Configuration of network elements discovers the network elements and maintains the topology such as adding, modifying and deleting in the network element configuration. Fault components normally deals with network element failures, physical failures and report failure details, service restoration and problem solution. Performance components deal with measure the network performance using metrics. Mediation components implement

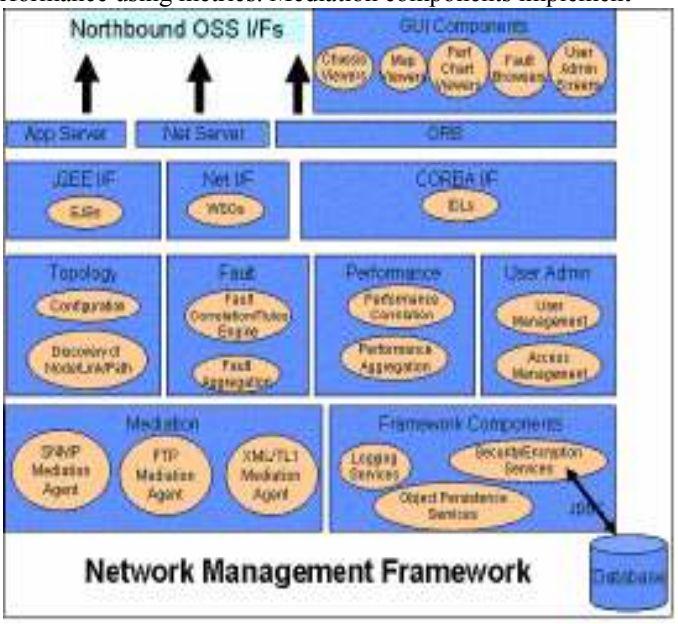

Figure 1: Traditional NMS Architecture [10]

specific protocol interface functionality on the southbound interface to communicate with the network elements. Frame components provide basic platform functionality, including, persistence, logging and security [10].

V. SNMP: ONE CRITICAL COMPONENT TO NETWORK MANAGEMENT & SECURITY

Network management requires end-to-end monitoring, controlling, and operation of network with using single management protocol or multiple management protocols.

Network management protocol is a simple application protocol in TCP/IP protocol suite. This piece of software used in most of the network elements. SNMP normally used to inspect the remote users in network. This protocol is used to communicate network management information between network management system and network elements in a network such as host, routers, scanners, hubs and for solving capability and interoperability problem [11]. It plays important role in monitoring the network. The protocols used for SNMP implementation are UDP, IP and TCP. Network monitoring and controlling tools are available based on SNMP, which are users friendly and more powerful it will work on wide range of operating systems [2].

There are three principal commands that an SNMP management station uses to obtain information from an SNMP agent:

1. The get command collects statistics on SNMP devices.

2. The set command changes the values of variables stored within the device.
3. The trap command reports on unusual events that occur on the SNMP device.

The SNMP management console reviews and analyzes the different variables maintained by that device to report on device uptime, bandwidth utilization, and other network details [27].

This application serves network management services such as configuration management, fault management and performance management.

SNMP is a unified solution for gathering and updating data all the devices and applications on your network, so it goes without saying that you must be careful in its implementation. Properly securing SNMP is critical. That security can occur through a range of tactics, including the use of access lists on firewalls to isolate SNMP traffic, ensuring that strong Community Strings are used to prevent hacking, leveraging the privacy and encryption

Functions that are available in SNMP v3, and/or the use of isolated management VLANs that are dedicated for SNMP communication. Any or all of these capabilities goes far in securing SNMP against the threat of external attack[4].

VI. TELECOMMUNICATION MANAGEMENT NETWORK

CCITT (now International Telecommunications Union (ITU)) recommendation X.7OO/ISO 7498-4 of OSI systems management describes the architecture of the telecommunication management network. The purpose of TMN is to provide a set of standard interfaces that will facilitate easy management of operations, administration and maintenance functions and network elements. TMN physical architecture addressed the TMN concept, reference points, interfaces and functional and physical models [8].

As telecommunication is a complex infrastructure spanning over network services, users, business entity. It defines a layered logical architecture are as follows [12].

Telecommunication network management model is as shown above in figure 2.

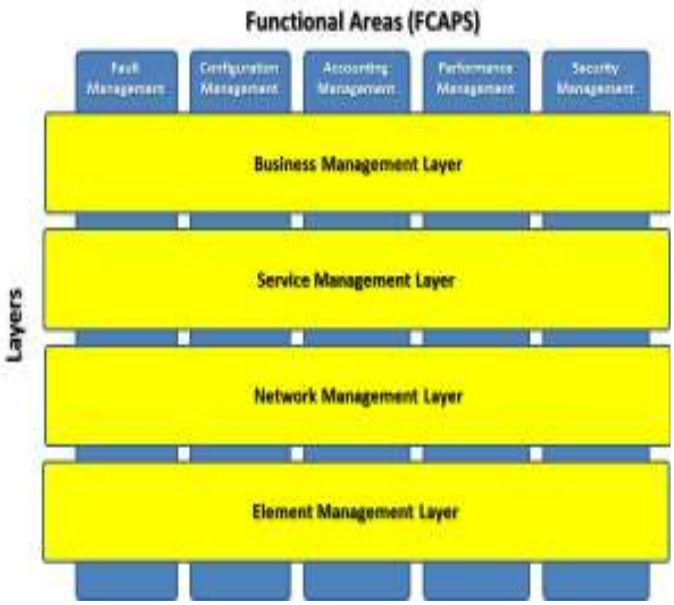

Figure 2: telecommunication network management model [12]

- Element management:
  Provides a view on a collection of network element usually forming a sub networks. Also mediates data between Network element & Network manager.
- Network management:
  Provides end to end network view of managed Resources & devices. It is device neutral.
- Service management:
  Provides contact with customer & service providers, Quality of service assurances, service order, billing Information & trouble ticketing
- Business management:
  Product & human resources planning. Business level view of service & financial concerns.

VII. MOBILE AGENTS FOR NETWORK MANAGEMENT

A. The need for agents in managing networks:

There is a trend towards increasingly heterogeneous networks in today's communications environment. Such diversity requires that network operators have greater knowledge and increased training. Managing these diverse networks requires the collection of large quantities of data from the network; data that must then be analyzed before management activity can be initiated. These challenges are the main forces driving research on software agents. Most of the research on the intelligence aspects of software agents comes from *Distributed Artificial Intelligence* (*DAI*) [13]. Distributed AI is an extension of ideas from Artificial Intelligence that applies to *Multi-Agent Systems* (*MAS*) [14]. Several centralized applications, each capable of addressing a certain aspect of a problem, can be tied together by a communication system. It would allow for exchange of their viewpoints and coming up

with strategies to make progress or to combine the results into a solution. This kind of problem solving is called *Distributed Problem Solving* (*DPS*) and each of the cooperating systems may be considered an agent. In Artificial Intelligence, an agent is viewed very often in terms of its *beliefs*, *desires* and *intentions* (so-called *BDI architecture*) [3].

B. Mobile agents

- Definition of software agent

It is a challenge to provide a definition of an agent that would not be controversial. One possibility is a definition of a software agent as a computational entity, which acts on behalf of others, is autonomous, proactive and reactive, and exhibits capabilities to learn, cooperate and move. This definition has its roots in the concurrent Actor model [15]. We will call these basic characteristics a basic agent model.

A mobile agent is a software agent that can move between locations. This definition implies that a mobile agent is also characterized by the basic agent model. In addition to the basic model, any software agent defines a life-cycle model, a computational model, a security model and a communication model. A mobile agent is additionally characterized by a navigation model. Mobile agents can be implemented using one of two fundamental technologies: mobile code or remote objects [3].

The size of mobile agents depends on what they do. In swarm intelligence, the agents are very small. On the other hand, configuration or diagnostic agents might get quite big, because they need to encode complex algorithms or reasoning engines. Note however, that agents can extend their capabilities on-the-fly, on-site by downloading required code off the network. They can carry only the minimum functionality, which can grow depending on the local environment and needs. This capability is facilitated by code mobility.

- Mobile Agent Framework (MAF) – An emerging standard

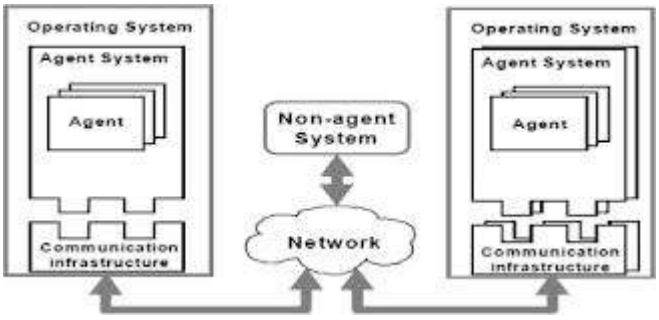

Figure 3: Mobile Agent Facility Architecture

As with any other communications-related activity, the general acceptance of mobile agents for network management activity will depend heavily upon standards.

The Open Management Group (OMG) has already begun work in the area of mobile agents.

The proposal identifies the need for mobile code regions, with gateways between them that provide an agent application virtual layer on top of the actual network. This architecture is shown in Figure 3. An agent region is defined as a set of agent systems that can access each other, possessing similar authority and identifying a default migration pattern. Mobile agent facilities include the storage and retrieval of agents, remote agent creation transfer and agent method invocation. The draft standard also draws heavily on CORBA, with IIOP being used as the transport protocol, and hinting that many pre-defined CORBA services, such as naming, may be used to support mobile agent activity.

- Network modeling

In Network Management, automatic discovery is one of the fundamental functions of the management system. We use an unqualified term on purpose, because discovery might target many goals. In the simplest case, just finding the devices of the network is of interest. Mobile code is a convenient vehicle for performing discovery tasks [17]. While basic network discovery (node discovery alone) is not a convincing justification for the use of mobile code, its more sophisticated variations certainly do benefit from the new capabilities. Nevertheless, the basic discovery of network devices is an excellent vehicle to illustrate the approach. One of the commonly used discovery techniques is sending ping messages to IP addresses in a certain domain. The discovering process builds its view of the network from the received responses. Instead, a mobile agent (a *deglet* – after a *delegation agent)* can be created with a sole task of sending the identifier of a visited node to the creator [18].

C. Advantages of mobile agents:-

The use of mobile agents may have advantages over other implementations of agents. This does not imply that other technologies (like remote objects) cannot be used instead, because virtually any task that can be performed with mobile agents can also be performed with stationary objects.

However, the traditional solutions might be less efficient, difficult to deploy, or awkward [3].

VIII. SECURITY IN NETWORK MANAGEMENT SYSTEM

Three key security layers required in management systems:

The first layer of NMS security is generally around AAA or Authentication, Authorization, and Auditing. Authentication is accomplished through a challenge-handshake mechanism where the credentials of the user are verified using a three-way handshake. The passwords are never sent across to the authentication module; rather a one-way-hash (called key) is used. This provides protection against playback attack using an incrementally changing identifier and a variable challenge value. Polices with strong password rules or the use of tokens can also be employed.

Once the user gets authenticated, he or she is given authorization for access control. The authorization policy is designed with "Fine-Grained Access Control" as the focus.
Auditing is about monitoring what the user does from the moment they sign in including the time and status of operation performed. This enables the network administrator to take necessary steps when an unauthorized execution is attempted by any user. Not only for security purposes, audit controls are extremely useful for debugging issues, for they allow you to determine what users were on the system before, during and after an incident so you can reverse engineer problems.
Device-to-Application Communications
The second layer of NMS/EMS protection is securing communications between the management application and devices across various protocols. Besides the secure protocol layers, the management system has various infrastructure components, each looking through various ports. The management system should be flexible enough to be able to assign non-standard port configurations, harden the system by design and be able to monitor port activity.
Inter-System Communication and Server Security
In the past, people figured that AAA and securing the device to the app pipe was sufficient protection. But to be truly secure today, inter-system communication is also vital. The NMS/EMS can be deployed in various environments where it needs to support different data stores depending on the requirements. Different data stores like Relational Database, XML, LDAP, NDS, etc., can be integrated. The security module provides administrative interfaces to configure the data store [20].

IX. RESEARCH ACTIVITY

A research on study of the drivers, issues, and priorities for network managers and network management tools, technologies, and practices conducted by ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) entitled Network Management: Megatrends in Technology, Organization, and Process [26].
There are a growing number of centers conducting research on mobile agents. Such pioneers in providing agent frameworks as GeneralMagic [22] and Dartmouth College [23] have been joined, and sometimes surpassed, by IBM [15], Mitsubishi (Concordia), ObjectSpace (Voyager) and others. Interesting research on applications of and the tradeoffs in using mobile code for Network Management has been conducted by the Computer Networks Group at Politecnico di Torino [21]. The Astrolog group at the Institut de Recherche en Informatique et Systemes Aleatoires (IRISA) uses mobile agents for the Mobile Network Manager (MNM) [24, 33]. This manager can be used from any location to manage a network remotely, for example, from a laptop connected through a modem.

CONCLUSION

This paper presents first Network management functionalities which play an important role in network management system. And also defines Network management Architecture. Then presents how SNMP is a critical component in Network management that provides valuable insight to any Network administrator who requires complete visibility into network & acts as a primary component of complete management system. Then discussed Telecommunication network management that provides for the structuring of the various management services. Then discussed the use of mobile agents for managing networks. Recent developments in the use of the Internet indicate that underline the importance of the agents in information intensive applications. Agent mobility is being increasingly used to perform various tasks that would otherwise require extensive attention spans by the users of the services provided on the Internet. Network management researchers should watch very closely the advancements in the Internet-based network computing technology, because the proliferation of this technology will be a driving force for designing better management systems. And at last discussed which are the three key security levels, and there functions in network management system.

REFERENCES

[1] Kumar, Prem G and Venkataram, P (1997) *Artificial intelligence approaches to network management: recent advances and a survey.* In: Computer Communications, 20 (15). pp. 1313-1322.
[2] Srinivas Basa & Naveen Ganji, "Enhanced NMS Tool Architecture for Discovery and Monitoring of Nodes", *Master Thesis Computer Science Thesis no: MCS-2008-15 January 2008.*
[3] Andrzej Bieszczad, Bernard Pagurek, Tony White , Systems and Computer Engineering, Carleton University, "Mobile Agents for Network Management, IEEE.
[4] www.solarwinds.com./SolarWinds_Network_Mgmt_Protocols.pdf.
[5] Markus Fiedler, "Network Management", Sub Model of Network Management Architecture, Department of Telecommunications, Blekinge Techniska Hogskola BTH, 15 Nov, 2007.
[6] Shane O'Donnell, "Network Management: Open Source Solutions to Proprietary Problems" 975 Walnut St, Suite 242, Nov 2000.
[7] N.B. Seitz, Performance standards for packet switched services. IEEE GLOBECOM, 1989, pp. 63-70.
[8] J. Milham, P. Dinesh, OMNIPoint-the implementation of version of telecommunication management networks, in: IEEE Network Operations and Management Symposium, Kissmmee, FL.
[9] Mani Subramanian, *Network Management: An Introduction to Principles and Practice*, ISBN 0-201-35742-9, Addison-Wesley, 2000.
[10] Venkatesan Krishnamoorthy, Naveen Krishnan Unni, V. Niranjan, " Event- Drivern Service-Oriented Architecture for an Agile and Scalable Network Management System", Computer Society, IEEE, 2005.
[11] Jeffery D. Case, James R. Davin, Mark S. Fedor, Martin L. Schoffstall, "Internet Network Management Using The Simple Network Management Protocol", IEEE.
[12] Raouf Boutaba & Jin Xiao, " Telecommunication System & technology-Vol II- Telecommunication nrtwork management.
[13] Vinoski, S., *CORBA overview: CORBA: Integrating Diverse Applications Within Distributed Heterogeneous Environments*, IEEE *Communications Magazine*, Vol. 14, No. 2.
[14] Gray., R. S., *Agent Tcl: A transportable agent system*. In Proceedings of the CIKM Workshop on Intelligent Information Agents, Baltimore, Md.
[15] Lange, D. B.,Oshima, M., Karjoth, G. and Kosaka, K. *Aglets:*

Programming Mobile Agents in Java In Proceedings of Worldwide Computing and Its Applications (WWCA'97), Lecture Notes in Computer Science, Vol. 1274, Springer Verlag.

[16] Cheng, D. T. and Covaci, S., *The OMG Mobile Agent Facility : A Submission*, in Rothermel, K. and Popescu-Zeletin, R., Eds., *Mobile Agents*, Springer-Verlag.

[17] Schramm, C., Bieszczad, A. and Pagurek, B. (1998), *Application-Oriented Network Modeling with Mobile Agents*. Proceedings of the IEEE/IFIP Network Operations and Management Symposium NOMS'98, New Orleans, Louisiana.

[18] Bieszczad, A. and Pagurek, B., (1998), *Network Management Application-Oriented Taxonomy of Mobile Code*, Proceedings of the EEE/IFIP Network Operations and Management Symposium NOMS'98, New Orleans, Louisiana, February 15-20, 1998.

[20] Security-in-network-and-element-management-system.aspx.

[21] Gosling, J. and Arnold, K., Joy, B., Steele, G., Lindholm, T., Walrath, K., Campione, M., Yellin, F. et al, *The Java Series*, Addison-Wesley.

[22] Kotay, K. and Kotz, D., *Transportable Agents*. In Yannis Labrou and Tim Finin, editors, Proceedings of the CIKM Workshop on Intelligent Information Agents, Third International Conference on Information and Knowledge Management (CIKM 94), Gaithersburg, Maryland.

[23] Gray., R. S., *Agent Tcl: A transportable agent system*. In Proceedings of the CIKM Workshop on Intelligent Information Agents, Baltimore.

[24] www.irisa.fr/solidor/work/astrolog.html

[25] Sahai, A., Morin, C. and Billiart, S., *Intelligent agents for a Mobile Network Manager (MNM)*. In Proceedings of the IFIP/IEEE International Conference on Intelligent Networks and Intelligence in Networks.

[26] Jim Frey, "EMA Research brief: Network management megatrends".

[27]Network instruments,"SNMP Monitoring: One Critical Component to Network Management" 2005.