マルチメディア通信と分散処理　62－7
（1993. 9. 20）

効率的なネットワーク管理のための情報，知性及びアルゴリズム

G. MANSFIELD*，K JAYANTHI*，木村 行男*，根元 義章†

* 高度通信システム研究所
† 東北大学

* 〒989-32 仙台市青葉区南吉成 6-6-3 ICR ビル
Tel: +81-22-279-3310 FAX: +81-22-279-3640 email: glenn@aic.co.jp
† 東北大学，仙台

あらまし

本研究で，我々は，ネットワーク管理に求められる情報について検討を行い，ネットワーク構成，ポリシー等の情報を付加することにした．これらの情報に基づき，効率的にネットワーク管理に関する決定を行なうアルゴリズムを提案した．

和文キーワード　ネットワーク管理，知的システム，アルゴリズム，構成管理

Information, Intelligence & Algorithms for Efficient Network Management

Glenn Mansfield*, K. Jayanthi*, Y. Kimura*
Y.Nemoto†

* AIC Systems Laboratories
† Tohoku University

*Advanced Intelligent Communication Systems Laboratories
6-6-3, Minami Yoshinari, Aoba-ku, Sendai 989-32, Japan.
Tel: +81-22-279-3310　FAX: +81-22-279-3640　e-mail: glenn@aic.co.jp
†Tohoku University,Sendai.

Abstract

In this work we have examined the information requirements of network management systems. We have enriched the information with configuration/ policy ... related details. Based on this information, we have proposed algorithms that can make decisions for efficient network management.

英文 key words　Network Management, Intelligence, Algorithms, Configuration Management

1 Introduction

Any management basically involves gathering information about the subject that needs to be managed. The gathered information is then processed and analyzed using the knowledge about the subject, to make judgements about the status of the subject and to take decisions about the future course of action.

Traditional network management systems which have concentrated mainly on monitoring network traffic, performance and fault detection have focussed on the operations and functions of the network elements and their interfaces. In the Internet there are several MIBS that are proposed standards or are under development- almost all relate to protocol layers 1-4.

However for efficient network management, it is important to *know* about higher level information e.g. the functioning of the applications and the network configuration, administration and policy.

Given the appropriate information intelligent management applications can be created by developing algorithms that model an expert network managers approach to solving a particular problem.

In Section 2 we present the network management framework that is currently widely used. In section 3 we examine the various information components of a management system. In section 4 we take a look at the algorithms that use the management information to ensure efficient management. We conclude with section 5.

In the rest of this work a *network* is the media for transmitting information. *network elements* are equipment with one or more *network interfaces* whereby it is possible to exchange information with the network. *Network elements* with multiple interfaces e.g. gateways/routers/bridges/repeaters... may be used to connect networks.

2 A Model for Intelligent Network Management

Most of the work in Network Management, so far, has been done in building the framework for collecting information from the network. Presently, there is an agreed management framework. Agents residing in network elements will provide the network manager application with information about the network. Standards have been fixed for communicating management information between the manager and the agent. The objects which need to be managed, are listed up and described in terms of their properties in MIB's. In this framework, the human managers' view of the network is limited to objects in the Management Information Base(MIB). Of course extensive research has been carried to develop these MIBs and the development and refinement is an ongoing process.

In the following discussion we will use the example of the SNMP [SNMPv2], [SMI], [MIB-II] network management framework; it is possibly the most widely deployed and experimented.

3 Information Components of a Network Management System

The Information Components of a network management system are as follows:

- Communication core component
  - System
  - Lower Layers
  - Network Layer
  - Transport Layer
- Application component
- Infrastructure component
  - Network configuration
  - Administrative
  - Policy

In the following section we briefly describe the issues related to various components.

3.1 Communication core component

This component is possibly the most widely explored discussed and deployed. The MIB-II [MIB-II] contains the core set of managed objects for a managed system's System, Lower, Network & Transport layers of the Internet suite of protocols. The Host Resources MIB is currently under development [HRMIB]. It covers the system and process related details of network elements. There are several other MIBs which deal with a specific type of interface or transport medium or protocol. Together these MIBs allow the monitoring and management of the communication infrastraucture - the lines nodes and the communication protocol entities. They give an immediate idea of the functioning of the network and are widely used for network monitoring, traffic and performance estimation, fault-detection, ...

3.2 Application

With the basic management framework reasonably well established and with the growing spread of network applications like mail, news, DNS, Directory Services, ... , the issue of managing Network Service Applications(NSA) is gathering attention. NSAs include all applications that provide network services. The necessity of managing Network Service Applications is particularly critical for NSAs which have (widely) distributed components such as the Mail and Directory Services.

The targeted NSA management centers around general monitoring

- to detect a broad range of operational problems: broken connectivity, system failure, congestion, ..
- to monitor performance and utilization

Presently a generic NSA-MIB [NSA-MIB] which covers the general network service related aspects. It focusses on the NSA description, the operations and activity indications, the associations and association related details and

two application specific MIBs for mail [MTA-MIB] and directory [DSA-MIB] applications which focus on the respective application-specific aspects are under development.

3.3 Network Infrastrauctures

The widening span of computer networking has highlighted the importance of holding and servicing information about the networking infrastructure itself. The growing and active interest in network management [GYM], is severely constrained by the lack of any organized pool of information about the network infrastructure itself. Some attempts have been made, on a piecemeal basis, to provide a larger view of some particular aspect of the network (WHOIS, DNS, .. in the case of the Internet; [WHOIS], [DNS]). Presently, there is a movement to explore the possibility of setting up a framework to hold and serve the infrastructural information of a network [ND].

3.3.1 Infrastructural information requirements

Network operation and management requires information about the structure of the network, the nodes, links and their properties & functions. Further, with current networks extending literally beyond bounds, the scope of the information covers networks beyond the span of local domain of authority or administration. When the Network was relatively small and simple the map was already known to the knowledgable network administrator. Based on this knowledge the course of the packets to different destinations would be charted. But presently the size of the Network is already beyond such usages, with the current growth being near explosive. This is giving rise to the urgent necessity of having infrastructural and service related information made accessible from all places and at all times in a reasonably efficient manner and with reasonable accuracy.

Network related information, referred to as 'network map' in the rest of this paper, should

1. Show the interconnection between the various network elements. This will basically represent the Network as a graph where vertices represent objects like gateways/workstations/ subnetworks and edges indicate the connections.
2. Show properties and functions of the various network elements and the interconnections. Attributes of vertices will represent various properties of the objects e.g. speed, charge, protocol, OS, etc. Functions include services offered by a network element.
3. Contain various name and address information of the networks and network elements.
4. Contain information about various administrative and management details related to the networks and network elements.
5. Contain the policy related information, part of which may be private while the other part may be made public.

Using this map the following services may be provided

1. Configuration management:
   - Display the physical configuration of a network, i.e. nodes and their physical interconnections
   - Display the logical configuration of a network, i.e. nodes and their logical interconnections.
2. Route management:
   - Find alternate routes by referring to the physical and logical configurations.
   - Generate routing tables considering local policy and policy of transit domains.
   - Check routing tables for routing loops, non- optimality, incorrect paths, etc.
3. Fault management: In case of network failures alternatives may be found and used to bypass the problem node or link.
4. Service management: Locate various services and servers in the Network.
5. Optimization: The information available can be used to carry out various optimizations, for example cost, traffic, response-time, etc.
6. Provide mappings between the various names and addresses of elements
7. Depict administrative/autonomous domains.
8. Network Administration and Management: References to people responsible for administering and technically maintaining a network will be useful.

Examples of such usages are described in [IP], [SPP], [CMAN].

3.3.2 Nature of the Network Map - The X.500 solution

Implementing and maintaining a detailed map of the network poses a serious problem. The scope of the map is global and the network itself is expanding. Some of the problems that are peculiar to the network map are listed below:

- The Network configuration is quasi-static. Nodes, links and networks are being added,updated and deleted someplace or the other.
- The Network is huge and geographically distributed.
- The Network spans several political and administrative areas. The related information is also controlled and maintained in a distributed fashion.

In short, global network configuration information is unwieldy and growing continuously. It is impossible to service such information in a centralized fashion. So, a distributed database system is necessary. In this context, the X.500 Directory system [X.500-88] is an appropriate candidate on which the network map may be implemented. The X.500 Directory is intended to be a very large and highly distributed database. It is structured hierarchically with entries arranged in the form of a tree in which each object corresponds to a node or an entry. Information is stored about an object as a set of attributes.

4 Algorithms

As can be expected a whole range of applications can be developed based on the information components provided. Simple monitoring of the network for fault detection, generating *annotated network maps*, making routing decisions, finding alternate paths in cases of failures or congestion, finding the *cheapest* source of a document are just some examples.

In this section we examine the various algorithms that may be used in some of these applications for efficient management.

4.1 Monitoring Algorithm

One of the purposes of network monitoring is to detect any abnormality or fault. This is the simplest of algorithms which involves the periodic checking of the value a managed object or a set of managed objects. The detection of abnormality or fault depends on the type and definition of the managed object. This is the cue to the MIKB approach to building network management knowledge bases.

4.1.1 Types of Managed Objects

An examination of the MIBs for TCP/IP based internets shows that MOs are basically of the types shown in Fig.1. Appendix A gives the break-up of the MO's for each type.

Status objects	These take values from an enumerated set
Counter objects	Monotonically increasing non-negative numbers
Gauge objects	Non-negative numbers which may increase or decrease but latch at a maximum value
TimeTicks	A measure of the time in hundredths of seconds since some epoch
Descriptive	Descriptive information - names, addresses, routes,...
Sequences	Combinations of some or all of above
Tables	Array of sequences

Fig. 1 MO types in MIB

The information content of various types of objects from the management point view is given below:

- Status : generally gives a direct indication of the state of a system; for example whether the status of an interface is 'UP', 'DOWN' or 'TESTING'
- Counters, Gauges : generally a measure of some quantity (e.g. input packets, output errors, Q-lengths, ..) that gives an indication of the performance and/or status of the system. There are generally allowable/normal values and when the values go beyond these thresholds, the situation calls for special investigation/action.For example, continued and rapid increase of traffic is cause for alarm.
- Descriptive objects, sequences, tables : Changes in these objects generally indicate some change in the network and may merit an investigation. For example a change in the routing table is indicative of the addition/deletion of some link somewhere. A deletion of a link is in turn indicative of some faulty gateway/interface.
- TimeTicks : measures the time since an event has occurred.

4.1.2 Derived information: Velocity, Acceleration & History

The current value of a MO is a valuable piece of information. It tells a knowledgeable person more than just the figure, but only when read in the context of the history of the object. The frequency at which the object representing the operational status of an interface is changing gives the operator an insight into the reliability/error proneness of the interface. The same holds for counter and gauge type objects.

interface is changing gives the operator an insight into the reliability/error proneness of the interface. The same holds for counter and gauge type objects. The information that some counter has a value x does not signify much when judged in isolation. The significance is seen by the manager by using the history of the object to estimate the time development of the MO. For example, it is crucial to know whether an error count is constantly increasing, rapidly increasing, or only transient. For a more quantitative analysis, it was clear that the *velocities* and the *accelerations* would be effective measures to capture time-development related derived information of Counter and Gauge type MOs.

The history of MOs are described in terms of Means, Medians, Modes, deviations, ... on a periodic basis (hourly/daily/weekly ..) and are retained in the Network Information Base (NIB), described in detail in section 3.6. These are indications of the patterns, if any, that the MOs are having in space and time and provide valuable indicators in determining the significance (normal/abnormal) of the current states of MOs.

4.1.3 Criteria for evaluating status

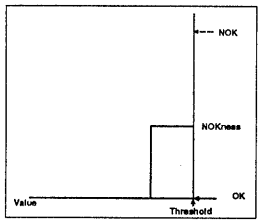


Fig. 2 The Step function

In the proposed model the network manager judges the status of the network by judging the information available (information, derived information, history) on objects against a status evaluation criteria which represents the managers' knowledge concerning the MO. This knowledge, MIKB, can be represented by the set $\{ C_i \}$ where C_i is the criterion to judge whether an MO indicates any abnormality in the network.

MIKB = $\{ C_i \}$

The abnormality a_i due to an object i is given by the criterion represented as a function as follows:

$$a_i = C_i(x_i, v_i, a_i, t_i)$$

where x_i is the value of the MIB variable, v_i is the velocity, a_i is the acceleration and t_i is the time interval in which the variable x_i is studied. The function C_i is a step

function (Fig.3a) which assumes the high value if x_i, v_i, or a_i exceeds their respective thresholds (for objects of type counter/gauge).

This was our basic proposal; but on our first interaction with the network manager we came across such statements like: *in the short term two packets lost per second is bad, and in the long term 60 packets lost per minute is bad.* This led us to refine our abnormality model to:

$$a_i = C_i(x_i, vs_i, vl_i, as_i, al_i, ts_i, tl_i)$$

where, vs_i, as_i, vl_i, al_i denote the velocity and acceleration in the short term and long term respectively, and, ts_i, tl_i define the time intervals for short term and long term respectively. The step function C_i assumes the high value if x_i, vs_i, vl_i, as_i or al_i exceed their respective thresholds and is low otherwise.

The composite abnormality of the system is then given by the *composition* of all the abnormalities:

$A = a_1 \oplus a_2 \oplus ... \oplus a_n$, where n parameters are being observed.

This leads us to a very simple means of quantitatively analysing the network status by ascribing thresholds to the counter, gauge type MO's and by ascribing status to the state variables.

4.1.4 Degree of abnormality

The knowledge represented in the model so far indicates whether the status of an MO is abnormal or not. There are several possible abnormalities in a network and not all of them are of the same degree of seriousness. An increase in the number of error packets would not warrant sending an alarm to the network manager to wake up that person in the middle of the night. However, the change of the operational status of an important network interface from "up" to "down", may warrant immediate alarm. Thus arose the necessity of assigning weights to each of the abnormal conditions. The weight represented the degree of seriousness of the abnormality of an MO. The weights themselves were functions of time. For example, if disk space is approaching criticality during a working day, since assistance is available at short notice, we can afford to wait longer. Whereas if it is weekend, then appropriate time must be given to allow the operator to reach and rectify the situation, which means that we cannot permit the critical situation to be actually reached.

4.1.5 Fuzziness of decision-making

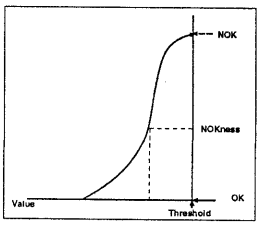


Fig. 3 The Fuzzy function

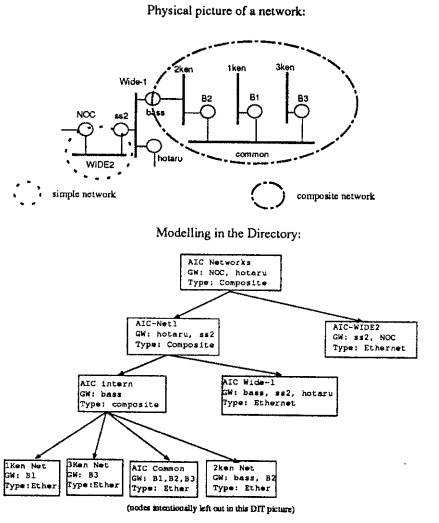
The other problem we faced with the abnormality was in evaluating threshold conditions. In the discrete mode of evaluation, if x_i or v_i is $\geq th_i + \alpha$, the sitution was deemed abnormal, while if v_i is ¡ th_i - α, the situation was deemed normal for however small α. This decision did not reflect the actual situation, and it did not find favour with the network managers, who preferred a more subjective decision like, if x_i is equal to th_i - α the situation is not "very" good (Fig.3).

Thus it was necessary to employ a fuzzy algorithm to compute the membership function that measured the *NOKness* of an MO, contrary to the step function C_i in sub-section 4.1.3.

For example, for a *Status* type object, if the value is a direct indication. For *Gauge* or *Counter* type objects there will be a reference value or threshold which decides whether there is an abnormality or not. E.g. the presence of error packets beyond a certain critical count would indicate a definite abnormaiity.

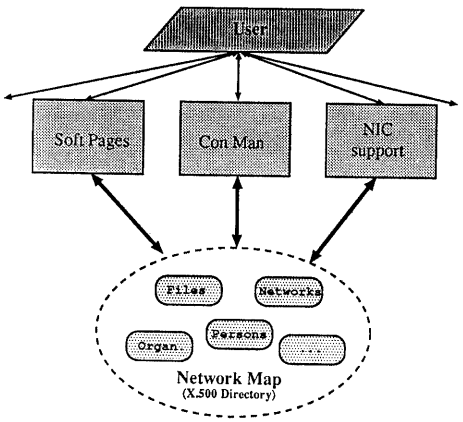
4.2 Network Maps

A map is very important for management purposes - irrespective of whether the manager is a human being or a application process. Given the configuration information is a straight forward generate the topological graph of the network where the vertices represent the components of the network and edges indicate the connections. For visual representation the graph may be translated to a more "physical" illustration.



Just as there are several maps of the same geographical domain (political, natural...) one can envisage several views of the same network and its components. A view (called "image" in the remainder) could pertain to a particular protocol suite (IP/OSI/...), an administrative domain or

purpose. Using images, several abstractions of the same object is possible (fig. 4).



4.3 Optimal Document Retrieval

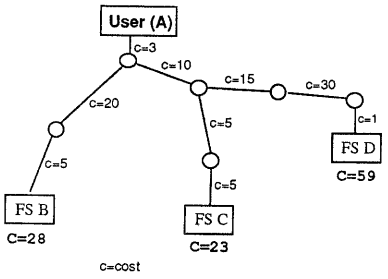


FIG. 5

It is desirable to query for files always on filestores that are nearest/cheapest to the users' site. For that purpose, it is necessary to evaluate distance/cost between the users' host and possible servers. Also, it is necessary to search the contents of the servers. For example, a user on host *A* looking for a certain document should under ideal situation carry out the search in the ordered list of fileservers *[C,B,D]*, the ordering being based on the potential retrieval costs. The Soft Pages Project [SPAGE] which implements this algorithm started with the wish to reduce ftp traffic on crowded overseas links and national backbones.

The algorithm makes use of the network infrastructure information concerning network configuration, location of servers and their contents, the links and their charges.

Parameter values are read from the network database and represent:

speed - the bandwidth (in kbps) theoretically available in a network

traffic - the average use (as percentage) of this network, thus telling something about congestion

charge - monetary units (as abstract integer number) to be paid for the transmission of one packet; this should be used to express relationship between several charges rather than absolut amount of money (not to speak of currency, exchange rates, etc.)

priority - sometimes system administrators want to keep certain connections free for important traffic like mails. They can do this by increasing the priority (integer value) of the network connection in comparison to another.

Cost is calculated as follows:

$$cost = f(speed, traffic, charge, priority)$$
$$cost = a*(1/speed)+b*traffic+c*charge+d*priority$$

whereas the weights a, b, c, d can be chosen freely by the administrator of a site. This way an individual evaluation is possible. For some sites speed has a higher weight than charge, for others it may be the other way around.

With the formula given above, a cost index can be calculated for one network connection. If traffic has to pass several networks, their cost indexes will be added to an overall cost index for the end-to-end connection. Thus, the number of network hops goes into the cost index, too.

4.4 Alternate Paths

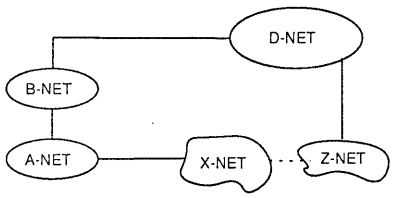


FIG. 7

Given the mesh-type connectivity of networks, it is very important to have a clear picture about the connections; for example, A-net has potential connectivity to D-net via multiple routes (fig. 7). The topological map of the network is useful; to find alternate paths in case of failure, to know the transit policy of the provider on the alternate path, to know the point of contact for the provider. Needless to say the map can be used to detect non-optimal routes and to evaluate the quality of the connectivity in terms of redundancy.

4.5 Fault Tolerant Management

This is a new topic that is coming up. In the present scheme a manager monitors networks thru the manager workstation. Now if the link from the manager workstation to the agent is down or still worse if the link to the managed network is down without alternate means there will be a collapse of network management. Among the alternate means are the following

4.5.1 Use Alternate paths for management traffic

This implies that the management application has control over the networking layer. It uses the network configuration information to decide the next alternative path/router and instructs the networking layer to route its requests/queries accordingly. The intelligent agent at the other end reads the request and sends the reply along the appropriate route.

4.5.2 Use Proxy Agents

This method is a more simpler method but involves the cooperation of a few more agents in the network. For example suppose the the link between management stattion A and Managed Station B is down. Now, if the link between A and some station C is up, and if there is a link between C and B, then if there is an agent on C which agrees to act as a proxy for the agent on B then the management station can redirect its query to the proxy agent on C.

5 Conclusion

The basic component of a network management system is the information that is fed into it. To complement the presently widely used information component - the application and infrastructure related component is proposed. As part of an effort to cope with the rapidly changing communications scene and the explosive growth in communication networks, the need for a framework to hold the infrastructural and service related information about communication networks has been emphasised. Algorithms to process the information components are discussed. The intelligence of a management system depends on the successful implementation of the algorithms. A Pilot based on this idea, presently covering the Japanese Internet, is in operation. Future plans involve extending the pilot to the International arena to cover other countries/NICs. The network model adopted in the Pilot for representing a communication network with all its related details and descriptions in the Directory, is described. A new genre of applications based on this proposal are coming up.

References

[SMI] Case, J., McCloghrie, K., Rose, M., and Waldbusser, S., "Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)", RFC1442, SNMP Research,Inc., Hughes LAN Systems, Dover Beach Consulting, Inc., Carnegie Mellon University,April 1993.

[MIB-II] McCloghrie, K., and Rose,M., Editors, "Management Information Base for Network Management of TCP/IP-based internets: MIB-II", STD 17, RFC 1213, Hughes LAN Systems, Performance Systems International, March 1991.

[SNMPv2] Case, J., McCloghrie, K., Rose, M., and Waldbusser, S., "Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)", RFC1448, SNMP Research,Inc., Hughes LAN Systems, Dover Beach Consulting, Inc., Carnegie Mellon University, April 1993.

[HRMIB] Grillo, P., Waldbusser, S., Host Resources MIB, Internet Draft, June, 1993.

[NSA-MIB] Freed, N., Kille, S., The Network Services Monitoring MIB, Internet Draft (work in progress), August 18, 1993.

[MTA-MIB] Freed, N., Kille, S., The Mail Monitoring MIB, Internet Draft, June 26, 1993.

[DSA-MIB] Mansfield, G., Kille, S., The Directory Monitoring MIB, Internet Draft, July 7, 1993.

[X.500-88] CCITT:
The Directory - Overview of Concepts, Models and Services;
Recommendations X.500 - X.521

[HK 91] Hardcastle-Kille, S.:
X.500 and Domains;
RFC 1279, November 1991.

[ND] G. Mansfield, et.al.
Mapping Communication Networks in the Directory
, Computer Networks & ISDN Systems (To be published).

[GYM] G.Mansfield et.al.
An SNMP-based Expert Network Management System
IEICE Transactions, August, 1992.

[IP] Johannsen, Th., G. Mansfield:
Representing IP information in the X.500 Directory;
Technical Report 92.8, AIC Systems Lab., Sendai, Japan, February 1993.

[SPP] Johannsen, Th., G. Mansfield:
The Soft Pages Project;
Technical Report 92.9, AIC Systems Lab., Sendai, Japan, February 1993.

[WHOIS] Harrenstein, K., M.K. Stahl, E.J. Feinler:
NICNAME/WHOIS;
RFC 954, October 1985.

[DNS] Mockapetris, P.V.:
Domain names - Concepts and Facilities;
RFC 1034, November 1987.

[FYI] FYI on a Network Management Tool Catalog;
Internet Request for Comments 1147, ed. R. Stine.;
April, 1990.

[FRE] D. C. M. Wood, S. S. Coleman, M. F. Schwartz;
Fremont: A System for Discovering Network

Characteristics and Problems;
Proc of Winter USENIX, San Diego, pp 335-348, January, 1993.

[CMAN] Configuration Management using the Directory Services;
G. Mansfield, K. Jayanthi, K. Higuchi, S. Noguchi;
Proc of the National Conf. of the Information Processing Society of Japan;
October 1992.

[SPAGE] The SoftPages Project;
Thomas Johannsen, G. Mansfield, K. Takahashi, S. Noguchi;
Proc of the National Conf. of the Information Processing Society of Japan;
October 1992.

[NIC] NIC Services using the Directory;
Glenn Mansfield, Thomas Johannsen, K Jayanthi;
Technical Report 92.10, AIC Systems Lab., Sendai, Japan, February 1993.