FDDI NETWORK MANAGEMENT SYSTEM - FAULT, SECURITY,AND EVENT MANAGEMENT

ABSTRACT

The Fiber Distributed Data Interface (FDDI) is a fiber-optic based token-ring architecture with a throughput of 100 Mbits/s. Network Management System (NMS) is the system which manages and controls the communication resources, and the FDDI NMS is based on FDDI ring. Along with the growth of FDDI devices has come the recognition of FDDI NMS as an important aspect of computer networking.

In this paper, we developed and described an FDDI NMS for assisting the network operator and analyst in understanding and controlling FDDI ring and its subnets. The FDDI NMS provides an integrated set of tools for real-time monitoring, control, and analysis of FDDI consisting of ethernets. It also provides mechanism for network security management which protects the NMS from unathorized use.

Key Words: FDDI, NMS, Fault Management, Security Management , Event Management.

I. INTRODUCTION

Within a given organization, the trend is toward larger, more complex networks supporting more applications and more users. As these networks grow in scale, two facts become evident: (1) The network and its associated resources and distributed applications become indispensable to the organization. (2) More things can go wrong, disabling the network or a portion of the network or degrading performance to an unacceptable level. A large network can not be put together and managed by human effort alone. The complexity of such a system dictates the use of automated network management tools (Stallings, 1990). The comminication medium is toward high speed transmission, such as FDDI. The FDDI provides a high bandwidth (100 Mbits/s) general puspose interconnection using fiber optics as the transmission medium. The FDDI design allows a maximum configuration of 1000 stations connected with 200 km of optical fiber. Its design specification calls for no more than 1 error in $2.5 * 10^{10}$ bits (Keiser,1989; Tanenbaum,1988). Along with the growth of FDDI devices has come the requirements for controlling and monitoring the complex and high speed FDDI networks. To control the resources and network status, a network management system is necessary. An FDDI Network Management System is expected to manage FDDI ring nodes and its subnets.

The OSI (Open Systems Interconnection) Management standards define Fault Management, Configuration and Name Management, Performance Management, Accounting Management, and Security Management. The aim of OSI Management standards is to allow interoperability and integration between the large number of products and services in today's information networks. It only defines framework and no protocol format details. So there are not any FDDI NMS standards between current FDDI NMS products. For understanding the details of FDDI NMS, such as protocols design, we choose to implement FDDI NMS. And then we can know the necessary protocols, improve them before the detailed FDDI NMS standards defined. Establishing Network Management standards is extremely challenging for four reasons (Caruso,1990): (1) The multitude of today's Network Management products were originally developed for the particular requirements of each vendor without anticipating the need to support open interoperability. (2) It requires careful and detailed work in defining the necessary open architecture, protocols, distributed management mechanisms, and structur-

ing of information exchanged in messages about managed components. (3) The work must be done so that minimum constraints are placed upon the way vendors and network service provider will implement standards. (4) Standards must be designed in a flexible manner that anticipates their evolution needs.

Network Management (Sethi, 1989) is still a hard problem (Cassel, Partridge and Westcott, 1989). Although management has been a subject of research since the earliest days of networking, it is still possible to build networks that can transfer data, but cannot be managed (Malik, 1990). SNMP (Simple Network Management Protocol) standard defines management information base (MIB) containing some useful information, but they are insufficient for FDDI network management. For managing FDDI nodes, the frames that out of SNMP MIB standards must be used. We have developed an FDDI Network Management System which is compatible with FINEX NMS (FINEX is the Fibronics line of FDDI controllers). The FX 8210 is the first product on the market that is based on FDDI technology, using a VLSI chip set (Fibronics 1988,1989). A system of FX 8210 units implements a MAC layer learning bridge function between an IEEE 802.3/Eithernet LAN over an FDDI backbone. The FX 8210 is part of Fibronics SYSTEM FINEX family of FDDI based products and accessories. The FDDI NMS is used to manage the FX 8210 on the FDDI backbone and the ethernets which are connected to the FX 8210.

In this paper we present an FDDI NMS we developed. This system covers three aspects: FDDI Fault Management, FDDI Security Management, and FDDI Event Management. The rest of this paper is organized as follows. Section II provides literature review of FDDI NMS, including OSI architecture. Section III deals with our implementation of our FDDI NMS; the function, the system architecture and protocol of the three aspects are explored. Section IV presents the conclusion.

II. LITERATURE REVIEW

A. FIBER OPTIC NETWORKS

FDDI is a high performance fiber optic token ring LAN running at 100 Mbps over distances up to 200 km with up to 1000 stations connected. It can be used in the

same way as any of the 802 LANs, but with its high bandwidth, another common use is as a backbone to connect copper LANs. The FDDI cabling consists of two fiber rings : a primary ring for normal operation, and a secondary ring for use as a backup of the primary one, for "wrapping" the network when isolating a faulty station, and for various recovery algorithms (Ross, 1989).

The ANSI FDDI defines SMT (Station Management) (ANSI, 1989) , which provides the control necessary at the station level to manage the processes underway in the various FDDI layers such that a station may work cooperatively on a ring. A variety of internal station configurations are possible (ANSI, 1989).

B. OSI MANAGEMENT ARCHITECTURE

OSI defines the following models in management environment (Klerer, 1988):

(A) The *organizational model* describes ways in which OSI Management can be distributed administratively across management domains and management systems within a domain.

(B) The *information model* provides guildelines for defining managed objects and their respective interrelationship, classes, attributes, actions and names. Case and Partridge (1989) diagram the Management Information Base (MIB).

(C) The *functional model* describes the management functional areas and their interrelationships, such as follows:

1. **Fault Management** – Fault management facilities allow network managers to detect problems in the communications network and the OSI environment.
2. **Configuration and Name Management** – Configuration management is the set of facilities which exercise control over, identify, collect data from and provide data to OSI resources for the purpose of assisting in providing a continuous operation of interconnection services.
3. **Performance Management** – Performance management facilities provide the network manager with the ability to monitor and evalute the performance of the system, network and layer entities.
4. **Accounting Management** – Accounting management is the set of facilities which enable charges to be set for the use of resources and costs to be identified for the use of those resources.

5. **Security Management** – Security management facilities allow a network manager to manage those services that provide access protection of his communcations resources.

OSI architecture also includes OSI Management Structure and Management Services. For more details, see ISO (1987).

C. FDDI FAULT MANAGEMENT

FDDI Fault Management facilities allow network managers to detect problems in the FDDI network. These facilities include mechanisms for the detection, isolation, and correction of abnormal operation.

Faults are to be distinguished from errors. A fault is an abnormal condition that requires management attention (or action) to repair. A fault is usually indicated by failure to operate correctly or by excessive errors. Certain errors (such as a single bit error on a communcation line) may occur occasionally and are not normally considerd to be faults (Feridun, Leib and Ong, 1988). It is desirable to automatically diagnose system malfunctions in a timely and efficient manner to reduce the impact of the faults and the testing procedures on the performance of the system (Sutter and Zeldin, 1988).

Two kinds of data are stored in the network model: static configuration data and dynamic status data. Dynamic status can only be retrieved from the devices themselves. It rarely makes sense to maintain this data in a database as it is typically relevant only on an exception basis (Zhan, Thanawastien, and Delcambre, 1988). Fault Management service must ensure that the problem is truly resolved and that no new problems are introduced. This requirement is called problem tracking and control. In the FDDI network, several station internal configurations are defined within SMT standard, with state machines provided to specify their operation.

D. FDDI SECURITY MANAGEMENT

FDDI Security Management facilities allow a network manager to manage those services that provide access protection of his FDDI communcations resources. The OSI Security Management provides support for the management of (ISO, 1987): (1) Authorization facilities (2) Access control (3) Encryption and key management (4) Authentication (5) The maintenance and manipulation of security logs.

Security management is one of the most difficult areas of network management to present, largely because those people who know the most about it are either reluctant or unable, for security reasons, to discuss it. A secure system can only be secure if you can trust that the protocols that manage it are not compromised. But the only way to ensure that the management protocols are not compromised is to make them secure (Cassel, 1989).

A system is secure if it adequately protects information that it processes. We say "adequately" because no practical system can achieve these goals without qualification; security is inherently relative (Witt, 1987). A secure system is multilevel secure if it protects information of different classifications from users with different clearances; thus some users are not cleared for all of the information that the system processes (Landwehr, Heitmeyer, and Mclean, 1984).

In 1977 the U.S. National Beraeu of Standards announced a Data Encryption Standard (DES). The encryption algorithm was developed at IBM and was an outgrowth of the Lucifer cipher designed by Feistel (Feistel, 1975; Denning, 1982). In 1978, Rivest, Shamir, and Adleman proposed a method for realizing public key encryption as suggested by Diffie and Hellman. The RSA algorithm makes use of the fact that it is easy to generate two large prime numbers and multiply them, but it is extremely difficult to factor the product.

A troublesome aspect of designing secure cryptosystems is key management. Even if the encryption algorithm is computationally infeasible to break, the entire system can be vulnerable if the keys are not adequately protected. Password files can be protected with one-way ciphers using a scheme developed by Needham (Morris and Thompson, 1979). A function f is a one-way function if, for any argument x in the domain of f, it is easy to compute $f(x)$, yet, for almost all y in the range of f, it is computationally infeasible to solve the equation $y = f(x)$ for any suitable argument x (Gong, 1989).

In pratice, users select short and easily remembered passwords. Such passwords are often simple to find by exhaustive search. Sequences of letters are systematically generated, enciphered, and then looked up in the table. In a study of password security on Bell Labs' UNIX, Morris and Thompson (1979) discovered that about 86% of all passwords were relatively easy to compromise. Since the TCP/IP protocols are popular, the security problems in the TCP/IP protocol suite are important for managing internetwork, and they are described by Bellovin (1989) and Kent (1989).

E. FDDI EVENT MANAGEMENT

Event Management consists of a set of utilities provided to visualize and analyze the changes and faults that occurred on a ring of FDDI stations, over a predefined period of time. These changes generate events that are recorded in the events database. Special filters can be applied when retriving the events, based on date, severity, codes, and sending stations.

Most of the polls are unnecessary (because the node is running properly) and it often takes some time to get around to polling a node after it develops a problem. Allowing a node to report a problem directly is more effective (Rabie, 1988). OSI defines Event Report Procedures, including confirmed and non-confirmed event-report procedures (ISO, 1987).

III. IMPLEMENTATION OF FDDI NMS

In this section, we describe the FDDI NMS taht we developed. The FDDI NMS is compatible with FINEX NMS (Fibronics, 1989). FINEX NMS is a proprietary software running on a PC AT or PS/2, that manages an FDDI ring composed of Fibronics FINEX stations. To run this system, setup the hardware and enter "NMS" in MS-DOS environment. The system is activated by user-invoked keystrokes, the significance of which depends on the screen being displayed. The various NMS facilities are reached through menus, starting from the Main Menu downwards to submenus and application screens. Since there are many menus in this system, we don't describe the menus here. Only the implementation of NMS services are presented, i.e., the user-interface design will not be discussed.

For being compatible with Fibronics station's NMS agents, we must send the same commands as the FINEX NMS do. So we must test what they send and do the backward-engineering to know how they work. From this, we find some improvements to the existing system. For lack of Fibronics support, we cannot implement these enhancement in the FINEX stations. The FINEX NMS implements many FDDI functions which are not defined in SNMP. For managing the FDDI nodes well, some services that out of SNMP standard are needed. The implementation helps us to know the details of NMS and is helpful for future NMS design.

A. System Architecture

The FDDI is used as a backbone on NTU campus network. Through FDDI backbone, we can communicate with any nodes in campus which are connected to it. The NMS is tested and run in the campus network. Each FINEX station contains specialized software dedicated to Network Management. It is through these "agents" (called "Systems Management Application Process — SMAP" in OSI terminology) that the NMS performs its functions. Thus, the NMS is a distributed system, composed of a network station (the manager, NMS) and the SMAPs (the agents, in FDDI nodes).

The NMS is connected to the FDDI nodes through RS232C serial I/O port. Although using RS232C, the performance of this system is acceptable. Only little data must be sent to and received from NMS agents, so the RS232C communication speed between NMS and FDDI nodes would not be a problem for current implementation. And using RS232C port can help us to control the network remotely through telephone line. This may be useful for wide-area network management.

The network can be operated without NMS. But it can help us to detect the problem and take the necessary actions to repair the network. From the system, we can know the status of the network, such as station up or down, and many information for manager to know what happens in the network. Through NMS, he needn't go to the physical location to find the faults, only from the NMS scrren can let us get many status in spite of the distance.

B. Management Services

The Network Management services are classified in three categories as follows:

(A) Data Manipulation Services – Two Services provide the capabilities for manipulating management data:

1. **GET** which allows for retrieval of data from management information database. The GET service is used to display parameters and status data from any FINEX station on the FDDI ring.
2. **SET** which allows for the modification of data in the management information database.

The following protocols use above presentation (GET,SET) to describe the data flow between NMS and FDDI nodes.

(B) Event Reporting Services – FINEX stations power on self-tests and any change on any FINEX station on the FDDI ring creat events that are reported to the NMS as they occur, or on a periodic basis, through the Event Reporting services. These event services may be activated or deactived but do not require polling to obtain information about events. The FINEX NMS only support non-confirmed event reporting service. Non-confirmed event needs less time, but being less reliable, and is only suggested for normal events. This may be improved by making confirmed-event for critical events.

(C) Direct Control Services – These services are used to request the performance of an action, that may permanently alter the state of the system, or usually, results in some transient behavior of the system. For example, when the system is requested to execute a certain diagnostic test.

The control service — ACTION enables to invoke an action and does not require confirmation. As above, the non-confirmed action may be dangerous for some actions, such as shutdown the station. So for important action, the confirmed action is required.

C. Frame format

For security reason, we only list some fields, and use symbolic equations to present the FINEX NMS encipher function in security management section. Since the FDDI product is still running now, sending the correct commands as the following may damage the network, such as shutdown the station which is prohibited by user. The common fields are in Table 1.

(A) For Fault Management Frames: Some of the the fault management frames use the SMT-like ones, since many fault management information are defined in ANSI SMT standards. For future development and being compatible with SMT, using SMT-like frames reserve more flexibility. For getting normal status, see Table 2. Table 3 shows SMT-function frame format.

(B) For Security Management Frames: The FINEX NMS has three levels of security control, each level user has one password for access control, and this is saved as a PC file. Using one-way cipher function to encipher the password, the hacker cannot find out the password esaily. For each FDDI node, there is one

Table 1: Common Field Format

Name	Size (byte)	Meaning
Start symbols	4	"s", X'14', X'56', X'78'
Frame class	2	frame class, function type
Sequence no	2	sequence no of request
Status	1	status of request
To	1	"to" field of this frame
Target Address	6	48-bit MAC address
DIU	2	number of LAN interface
Password	2	password
Control	6	perform special function
Information	N	information sent or received
End symbol	1	"e"
Checksum	2	adding from X'14' to "e" equals to 0

Table 2: Fault Management Frames

Function	frame class
Get PHY status	X'00 33'
Get 8410 status	X'00 33'
Get MAC counter	X'00 0F'

Table 3: SMT-function Frame Format

Function	SMT frame class	SMT frame type
SIF request	X'03'	X'02'
ECHO frame request	X'04'	X'02'

Table 4: Security Management Frames

Function	frame class
Citynet Group Manager	X'00 5E'
FDDI user	X'00 5C'
Network Manager	X'00 5A'
Field Engineer	X'00 5B'

password for each level. To send commands, the local password must be same as the FDDI node's one. So there may be a problem when we change the local password but not changing the FDDI node's one. This can be improved easily by a double checking algorithm. For being compatible with FINEX stations, we must guess the true encipher function and set the correct values in the sending frame to communicate with FDDI agents. Then futher enhancements can be done. By common sense, it is difficult for anyone to find out the encipher function, and needs many efforts. Through a planned guessing method, we find out the true encipher function finally. The guessing process can help us to design a better encipher function which is much difficult to guess, since a better encipher function design must be doned with how to discover it. For setting passwords of FINEX stations on the FDDI ring, see Table 4.

(C) For Event Management Frames : When a node detects an anomalous condition (for example, a routing loop or a defective link), it sends an event message to NMS. Each event may be assigned a two-part value:

1. The *event code* is a code that indicates the general type of problem. Event codes have the same meaning across all nodes. For example, event code might be "NC", "NS", ..., for different types of events.

2. The *event number* is an implementation-specific value that uses to further classify the event. For example, "NC109" means "Local starts responding."

The FINEX NMS only support non-confirmed events, and the format of this frame is as follows: (1) frame class = X'01 36' (2) sequence no = X'00' (3) status = X'07'.

Table 5: Meaning of variables

name	meaning	content
l	Length of password string	5 ... 20
S	password string	$S_1 \ldots S_l$
CB	Code Base	$CB_5 \ldots CB_{20}$
PV	Positional Value	$PV_i = S_i - '0'$
IV	Interval Value	$IV_1 \ldots IV_{20}$
AV	Adjust Value	$AV_1 \ldots AV_{20}$
AV1	Adjust Value 1	$AV1_{'0'} \ldots AV1_{'Z'}$
CAV	Code Adjust Value	$CAV_5 \ldots CAV_{20}$
SV	Shift Value	X'000E'

D. FINEX NMS Encipher Function

The FINEX NMS uses a one-way cipher function for enciphering password string to two byte code. The function is consisting of four parts which are presented as follows. Legal characters set are: 0, 1, ..., 9, A, B, ..., Z. The lowercase alphabet would be translated to uppercase one. The meaning of variables are shown in Table 5.

$$CB_l \tag{1}$$

$$\sum_{i=1,i\neq 5}^{l} PV_i * IV_i \tag{2}$$

$$\sum_{i=1,i\neq 5}^{l} PV_i * AV_i * PV_5 \tag{3}$$

$$CAV_l * PV_5 + \begin{cases} PV_5 * (PV_5 - 1) * SV/2 & \text{if } l = 5 \\ AV1_{S_i} & l \neq 5 \end{cases} \tag{4}$$

Enciphered code = (1) + (2) + (3) + (4)

E. FDDI Fault Management

Fault management facilities allow network managers to detect problems in the FDDI network. It provides the procedures to: (1) Report the occurrence of faults. (2) Log the reported errors and failures in an error log for future analysis. (3) Schedule and execute diagnostic tests, trace faults and initiate the correction of faults.

During the diagnostic process, the network model is manipulated and updated as more information is gathered from the network concerning a specific problem. System level faults are assumed to occur either at a node or at a link. Faults at a node cause it to fail-stop or are detected by the node's built-in-test procedures. The NMS monitor will diagnose the system faults by transmitting a sequence of Diagnostic Messages to various nodes on the FDDI ring and by examinig the response.

There are two types of fault management: Diagnostics facilities and Reset & Recovery facilities. They are described as follows:

(A) Diagnostics facilities

1. **Display PHY Status** – This function monitors the current PHY configuration of the target station.

   Protocols

   (1) The NMS requests to retrieve the PHY status from the target station by issuing a GET-PHY request.

   (2) The target station retrieves the PHY status or rejects the GET-PHY request by issuing an GET-PHY response.

2. **Display FX8410 Status** – The function presents the status of the two FX8410 units adjacent to the target station, if any.

   Protocols

   (1) The NMS requests to retrieve the status of FX8410 from the target station by issuing a GET-FX8410 request.

   (2) The target station retrieves the FX8410 status or rejects the GET-FX8410 request by issuing an GET-FX8410 response.

3. **Display MAC counters** – This function displays various hardware and software counters that provide useful diagnoatics infomation.

   Protocols

   (1) The NMS requests to retrieve the MAC counters from the target station by issuing a GET-MAC-CNT request.

   (2) The target station retrieves the MAC counters or rejects the GET-MAC-CNT request by issuing an GET-MAC-CNT response.

4. **SIF operation request[SMT]** – The Status Information Frame (SIF) operation request is uesed by the NMS to retrived information about operation of the MAC in the target station.This request can be sent to any FDDI station that supports the SMT standard, even if it is non-Fibronics.

   Protocols

   (1) The NMS requests to retrieve the SIF counters from the target station by issuing a GET-SIF request.

   (2) The target station retrieves the SIF counters or rejects the GET-SIF request by issuing an GET-SIF response.

5. **Echo Frame Request[SMT]** – The Echo Frame Request is used by the NMS to verify transmission validity. The NMS send a test frame to target station requesting its echo. The echoed frame is then checked.

   Protocols

   (1) The NMS requests to echo the frame from the target station by issuing a ECHO request.

   (2) The target station echo the frame or rejects the ECHO request by issuing an ECHO response.

(B) Reset & Recovery facilities

1. **Warm Reset (no selftest)** – The function results in the station initialization without running the self-test.

   Protocols

(1) The NMS requests to initialize (warm reset) the target station by issuing an ACTION-WARM-RESET request.

(2) The target station initializes (warm reset) or rejects the request, no response frame.

2. **Cold Reset (selftest)** – The function is equivalent to hardware reset of the station, and is followed by station initialization with running the self-test procedures.

Protocols

(1) The NMS requests to initialize (cold reset) the target station by issuing an ACTION-COLD-RESET request.

(2) The target station initializes (cold reset) or rejects the request, no response frame.

F. FDDI Security Management

Security management facilities allow a network manager to manage those services that provide access protection of his communication resource. Security Management provides support for management of (1) Authorization facilities, and (2) Access control. Many access controls incorporate a concept of ownership, that is, users may dispense and revoke privileges for objects they own. The effectiveness of access controls rests on two premises: (1) Proper user identification – no one should be able to acquire the access rights of another. This premise is met through authentication procedures at login. (2) Information specifying the access rights of each user is protected from unauthorized modification. This premise is met by controlling access to system objects as well as user objects.
The security management procedures are described as follows:

(A) **Change User Class** – The function is used to change user's class. The three available user classes are: (1) User, (2) Network manager, and (3) Field Engineer.

(B) **Change User Password** – The function is used to change the user's password.

(C) Set Target Password – The function is used to update the station's passwords. The four available user classes are: (1) Citynet Group Manager, (2) FDDI User, (3) Network manager, and (4) Field Engineer.

Protocols

1. The NMS requests to set passwords on the target station by issuing a SET-PASSWORD request.
2. The target station sets the password or rejects the SET-PASSWORD request by issuing an SET-PASSWORD response.

G. FDDI Event Management

Event Management is not a seperate aspect of OSI NMS. It is a common service for the five aspects to use. The FINEX NMS supports more functions for manipulating events. It provides a set of utilities used to visualize and analyze the events which occurred on a ring of FINEX stations, over a predefined period of time, as recorded in the event database. The NMS recorded events belong to four categories: (1) Events resulting from processing of Event Notifications which are sent by each FDDI station on the ring upon its Power On, and as a result of changes, errors, or recovery detected during operation. (2) Events resulting from the diagnostic requests sent by the NMS to each FDDI station on the ring, at predefined, user settable intervals. (3) Reports originating at the NMS whenever it detects exceptional conditions. (4) Power up seft-test reports originated by the local FDDI station during power on.

There are many functions to support event management, such as follows:

(A) Display Events – The Display Events function is used to display the whole Event Log File, or a sub-set of events, as defined by the user through the filter facility.

(B) Display Backup Events – The Display Backup Events function displays a backup event file.

(C) Erase Events – The Erase Events function is used either to clear the whole Events Log File or to erase from the Events Log File all the events dated before a user entered date.

(D) Backup Events – The Backup Events function is used to backup the whole Event Log File or sub-subsection of events through the filter facility.

(E) Print Events – The Print Events functions is used to print events.

(F) Event Option – The Event Option is used to setup background related to the handling of the Event Log File.

The above Event Management services help us to management events, especially for large account of events.

IV. CONCLUSION

In the early 1990s, high-speed LANs based on fiber optics and FDDI standards are expected to be widely available. The LAN that installed today continues to work and interconnects to the FDDI cables, which act as very high-speed backbones. Computers with very high I/O data requirements may also attach to the FDDI LAN. In such an environment, FDDI NMS becomes critical to the success of the network. For this reason, we developed an FDDI NMS. Within a given organization using such configuration, we can use NMS to manage the network. The manager can get network information through NMS, and it is useful especially for those companies which having wide-area network.

In this paper, we developed and described a FINEX NMS compatible network management system. For being compatible with FINEX NMS, we can only develop the NMS under the architecture of FINEX NMS. Many new ideas cannot be implemented due to the lack of FX 8210 support. From the start, we had only FINEX NMS user's manual. After running, monitoring, matching, and guessing the frame format had come our NMS. It is passed through many tests, and works well for all functions that FINEX NMS supports for the three aspects. The encipher function of FINEX NMS is found by us; from this, we can see that there are still many problems of security management in FINEX NMS. It can help us to avoid easy breaking in future encipher function design, and that is the most important part in security management. Since there are no domestic FDDI NMS products now, the implementation helps us to know NMS thoroughly, and gets

the promotion of internal NMS technologies. And it makes us be able to find out better solutions for FDDI NMS implementation and protocols design, which are desired for domestic FDDI NMS design.

In this paper, we pointed out some means to enchance the management capabilities. Others may include the building of experts that can handle internetwork problems, including FDDI nodes. We hope that the FDDI NMS we proposed in this paper will lead to further discussion on the design of FDDI Network Management Systems.

REFERENCES

ANSI. *FDDI Station Management (SMT)*. ANSI X3T9.5. 1989.

Bellovin, S. M. Security Problems in the TCP/IP Protocol Suite. *ACM Communication Review* 19(2). 1989: 32-48.

Caruso, R. E. Network Management: A Tutorial Overview . *IEEE Communications Magazine* 28(3). March 1990: 20-25.

Case, J. D. and C. Partridge. Diagrams: A First Step to Diagrammed Management Information Bases. *ACM Communication Review* 19(1). 1989: 13-16.

Cassel, L. N., C. Partridge, and J. Westcott. Network Management Architectures and protocols: Problems and approaches. *IEEE Journal on selected areas in communications* 7(7). September 1989: 1104-1113.

Denning, E. D. *Cryptography and Data Security*. C.A.: Addison-Wesley Publishing Company, 1982.

Feistel, H., W. A. Notz, and J. L. Smith. Some Cryptographic Techniques for Machine to Machine Data Communications. *Proceeding IEEE* 63(11). November 1975: 1545-1554.

Feridun, M., M. Leib, M. Nodine, and J. Ong. ANM: Automated Network Management System. *IEEE Network* 2(2). March 1988: 13-19.

Fibronics. *FX8210 Technical Overview*. Fibronics Publication MA-9897, October. 1988.

------. *FX8510 FINEX NMS User's Manual*. Fibronics Publication MA-9752. September 1989.

Fong, K. and J. Reinstedler. The Development of an OSI Application Layer

Protocol Interface. *ACM Communication Review* 19(3). 1989: 21-58.

Gong, L. Using One-Way Functions for Authentication. *ACM Communication Review* 19(5). 1989: 8-11.

Grant, L. DES Key Crunching Safer Cipher Keys. *SIG. Security Audit and Control Review* 5(3). 1987: 9-16.

ISO. *Management Information Service Definition– Part 1: Overview.* ISO/DP /9595/1/N1372. February 1987.

------. *Management Information Service Definition– Part 2: Common Management Information Service.* ISO/DP/9595/2/N1373. February 1987.

------. *Management Information Protocol Definition– Part 1: Common Management Information Protocol.* ISO/DP/9596/2/N1376. February 1987.

Keiser, G. E. *Local Area Networks.* N.Y.: McGraw-Hill Book Company, 1989.

Kent, S. Comments on "Security Problems in the TCP/IP Protocol Suite". *ACM Communication Review* 19(3). 1989: 10-19.

Klerer, S. M. The OSI Management Architecture: an Overview. *IEEE Network* 2(2). March 1988: 20-29.

Landwehr, C. E., C. L. Heitmeyer, and J. Mclean. A security Model for Military Message Systems. *ACM Transaction on Computer Systems* 2(3). Auguster 1984: 198-222.

Malik, A. K. Network Management and Control Systems and Strategic Issues. *IEEE Communications Magazine* 28(3). March 1990: 26-29.

Morris, R. and K. Thompson. Password Security: A Case History. *CACM* 22(11). November 1979: 594-597.

Rabie, S. DAD: A Real-Time Expert System for Monitoring of Data Packet Networks. *IEEE Network.* September 1988: 29-34.

Rivest, R. L., A. Shamir, and L. Adleman. On digital signatures and public key cryptosystems. *CACM* 21. February 1978: 120-126.

Ross, F. E. An overview of FDDI: The Fiber Distributed Data Interface. *IEEE Journal on Selected Areas in Communications* 7(7). September 1989: 21-35.

Sethi, A. S. Bibliography on Network Management. *ACM Communication Review* 19(3). 1989: 58-75.

Sherer, J. R. and Murray, T. A. Management of the Intelligent Network. *IEEE Communications Magazine* December 1988: 21-24.

Stalling, W. *Business Data Communications.* N.Y.: Macmillian Publishing Company, 1990.

Sutter, M. T. and P. E. Zeldin. Designing Expert Systems for Real-Time Diagnosis

of Self-Correcting Networks . *IEEE Network.* September 1988: 43-51.

Tanenbaum, A. S. *Computer Networks.* N.Y.: Prentice-Hall International, Inc., 1988.

Witt, M. and N. Lewis. Specifying the Security Properties of Communication Systems. *SIG. Security Audit and Control Review* 5(3). 1987: 20-23.

Zhan, W. D., S. Thanawastien, and L. M. L. Delcambre. SIMNETMAN: An Expert Workstation for Designing Rule-Based Network Management Systems. *IEEE Network.* September 1988: 35-41.

光纖網路管理系統——障礙，安全，與事件管理

Chang-Sung Yu and Wu-Yao Cheng

游張松・鄭武堯

摘　要

光纖分散式數據界面(Fiber Distributed Data Interface; FDDI)是以光纖爲傳輸媒介，記號環 (token ring)架構並且每秒有一億位元的傳輸速率。網路管理系統(Network Management System; NMS)是管理及控制網路上資源的系統，而光纖網路管理系統就是以光纖網路爲主的管理系統。隨著光纖網路裝置的增加，使我們了解到光纖網路管理系統是電腦網路上的一個重要領域。

本文介紹我們發展出來的一個光纖網路管理系統，它能幫助網路操作員和分析者了解和控制整個光纖網路及其予網路。光纖網路管理系統提供了整合性的工具於即時監聽、控制和分析光纖網路系統，而且也提供了一套用於網路安全管理與控制的架構，以防止系統被未經授權者使用。