AN ABSTRACT OF THE THESIS OF

Yue-peng Zheng for the degree of Master of Science in Electrical and Computer Engineering presented on Dec 15, 1986

Title: A Simple Local Area Network COLAN --Control Oriented Local Area Network

Redacted for privacy

Abstract approved: ______________

James H. Herzog

COLAN (Control Oriented Local Area Network) is a redesign of the Task-Master, a daisy-chain structure distributed control system. COLAN is a simple bus structure communication subnetwork intended for distributed control applications. Low cost and simplicity are two main design criteria. Point-to-point and broadcast communications are possible. A packet switching technique is employed for data communication.

A fully distributed and "fair" channel access control protocol is developed for COLAN. It is a hybrid protocol which combines the CSMA/CD technique and the Token Bus technique. This control mechanism achieves high performance by changing between the CSMA/CD technique and the Token passing technique according to the load of the network. When the load of the network is light, COLAN employs the CSMA/CD technique. When the load is heavy, it uses the Token passing technique. It is believed that this hybrid control protocol will have a better performance than either the pure CSMA/CD technique, or the pure Token passing

technique.

A SIMPLE LOCAL AREA NETWORK

COLAN (Control Oriented Local Area Network)

by

Yuepeng Zheng

A THESIS

submitted to

Oregon State University

in partial fulfillment of
the requirement for the
degree of

Master of Science

Completed December 15, 1986

Commencement June 1987

APPROVED:

Redacted for privacy

Associate Professor of Electrical and Computer Engineering in charge of major

Redacted for privacy

Head of Department of Electrical and Computer Engineering

Redacted for privacy

Dean of Graduate School

Date thesis is presented December 15, 1986

Typed by Yuepeng Zheng for Yuepeng Zheng

Acknowledgement

I am grateful to my major professor, Dr. James H. Herzog, for his continuous guidance throughout this thesis and my graduate study at Oregon State University during last two years. There is no word which can express my deep appreciation to his through thesis readings and fruitful suggestions.

I also wish to thank my thesis committee members, Dr. R.S. Engelbrecht, Dr. L.C. Jensen, and Dr. T. Minoura, for their through thesis reading and fruitful suggestions.

I finally wish to thank the Asia Foundation for the financial support, and Dr. V. Young and other people of the Asia Foundation for their constant help.

I dedicate this thesis to my parents.

TABLE OF CONTENTS

LIST OF FIGURES

A SIMPLE LOCAL AREA NETWORK

COLAN -- Control Oriented Local Area Network

CHAPTER 1 INTRODUCTION

At present, information has become a vital resource comparable to food and energy. With the fast development of computer and communication technologies, office automation and manufacturing automation have become the keys to survival of a great many financial institutions and industrial concerns. With the concerns of low cost and high performance, distributed processing and computer networking technologies have been in use for more than a decade. Distributed processing systems and computer networks make information collecting, processing, transmission, and utilization much more efficient. Real-time control in industrial environments also requires distributed processing and computer networking.

1.1 Local Area Networks

With the rapid development of LSI and VLSI technologies, computer hardware costs have decreased dramatically and are accompanied by increased capability. The invention of the microcomputer brought computer power into offices and manufacturing fields and has influenced computer applications enormously.

Twenty years ago, computers could only be afforded by large organizations, the minicomputers of the seventies were purchased by departments and groups within such organizations. Now the personal computer is within the reach of every individual. Microcomputers have a much better cost to performance ratio than mainframes. They can be networked into a multiprocessor system. Compared to the equivalent capacity mainframe, this multi-processor system has the advantages of low-cost, high reliability and availability. Each user can have his or her own personal computer which is available at any time and also has a better response time than dumb terminals on mainframes. Because every microcomputer can operate independently, the failure of one or more microcomputers will not result in the failure of whole system.

With these advantages, more and more personal computers (microcomputers) are brought into office, manufacturing and home environments. Even though the cost of data processing hardware has dropped greatly, the cost of essential electro-mechanical equipment, such as mass storage devices and high quality line printers, still remains high. It is not feasible to provide large capacity disc drives and high quality line printers for each personal computer. Therefore, sharing these expensive resources is necessary.

All these developments result in a rapidly expanding area in computer technology, Local Area Networks (LANs). The definition of LAN, as given by Stallings [STAL 84], is that:

> A local area network is a communications network that provides interconnection of a variety of data

communicating devices within a small area.
Here the communicating devices include computers, terminals, peripheral devices, sensors (temperature, humidity, security alarm sensors), and so on.

Some of the typical characteristics of local area networks are:

* High data rate(0.1 to 100 Mbps)
* Short distance(0.1 to 25 km)
* Low error rate(10^{-8} to 10^{-11})

Local area networks have been under development for the last ten some years. There are many LANs commercially available such as Ethernet, IBM Token Ringnet, and Wangnet.

In the progress of office automation and manufacturing automation, LANs have played a very important role and will continue doing so.

1.2 COLAN: A Simple Control Oriented Local Area Network

1.2.1 Statement of Problems and Research objectives

The idea of developing COLAN was motivated by the effort to modify a single board computer, the Task-Master by Agile Systems, into a distributed network. The Task-Master is a daisy-chain structured multi-processor system intended for distributed control applications. It has the configuration shown in Fig.1-1. It consists of a Host, Task-Masters, a communication channel, and other devices (such as printers, temperature sensors, etc.). The Host is typically a personal computer, and is responsible for supervising the operation of the system. The host may send a command to a Task-Master instructing it to collect the temperature data, poll a Task-Master to see if there is security problems, and so on.

The Task-Master is a single board microcomputer based on an Intel MCS-48 microcomputer chip. The communication channel connects the Host and the Task-Masters together and it meets the EIA-RS-232C standard using twisted wire pairs. The system adopts centralized control for access to the communication channel. The outstanding characteristic of the Task-Master is its simplicity and low cost. These, in turn, present the system with some problems:

* Daisy chain structure: the open daisy chain structure determines that data can flow only in one direction; from the controller to the host. This makes it easy to implement since communication can happen between the system controller and a control node but not between pairs of control nodes.
* MCS-48 microcomputer chip: the MCS-48 family microcomputer chips are functionally very weak compared with todays' microcomputer chips. They have very limited program memory space and data memory space, the program memory space is only 4k bytes and is divided into two memory banks. All of these limit the further development of the system.

* RS-232C: The RS-232C standard has very limited range of transmission (the distance between the transmitter and the receiver can not be greater than 15 meters (50 feet)). This limits the system to be distributed in a rather small area. The transmission rate is also not high enough to assure efficient communication.

This research will address the redesign of the system so that it will have improved performance. The new system will be a simple local area network that is suitable for control applications and also suitable for being used as a communication system allowing devices in the system to communicate with one another.

1.2.2 Overview

The proposed system, which is called COLAN (Control Oriented Local Area Network), will be a single bus structure local area network. It will have the following features:

* Bus structure: COLAN will adopt a bus topology in which data can flow between any pair of devices and can also be broadcast to the network and received by all devices. The network will adopt a distributed control scheme for controlling the operation of the system. Distributed control of the system makes the system more reliable.
* MCS-51 microcomputer: the new system will use the Intel MCS-51 microcomputer chip to build the

network interface unit. This microcomputer chip is much more powerful than the MCS-48 family chips. It has a 64k data memory space and 64k program memory space and many other features for convenient programming. Its instruction set is larger and more powerful than the MCS-48.

* RS-485: The bus will meet the EIA standard RS-485. This standard has the advantages of longer transmission distance ability (up to 1.2km, or 4000 feet), higher data transmission rate, and uses a single power supply.

In the design of COLAN, simplicity and low cost, rather than very high performance, are the main criteria. COLAN will adopt a hybrid medium access control protocol which is the combination of the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) and Token Bus protocols. It is believed that this hybrid protocol will have better performance than either CSMA/CD or Token Bus. COLAN has the configuration as shown in Fig.1-2.

1.3 Organization of Dissertation

The first chapter of this dissertation has served as an introduction to the development of local area networks and COLAN.

Chapter 2 reviews local area networks. It first introduces the OSI (Open System Interconnection) Reference Model, then discusses ring LAN technologies, and follows with a discussion of bus LAN technologies.

In chapter 3, details of the COLAN organization are discussed. It discusses the bus structure, the switching mechanism, and the control mechanism of the COLAN. Chapter 4 is devoted to the discussion of the design of the COLAN. Its first section discusses the design of the control mechanism, the second describes the data link format, and the third discusses the design of the network interface unit.

Chapter 5 begins with the summary of COLAN, and it concludes in some suggestions for further development.

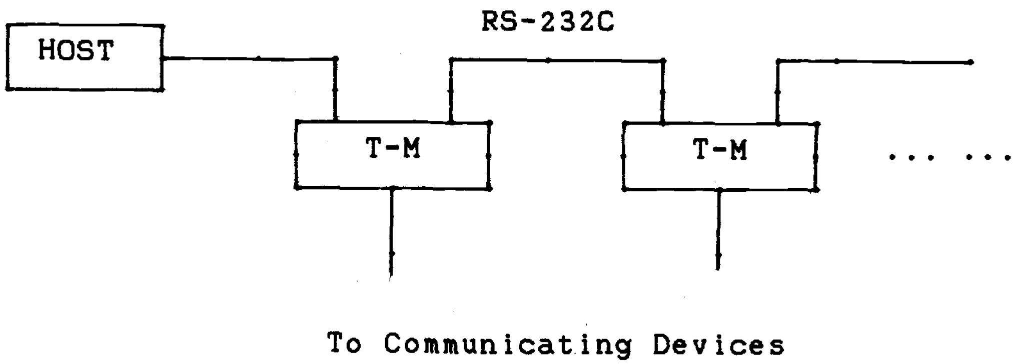
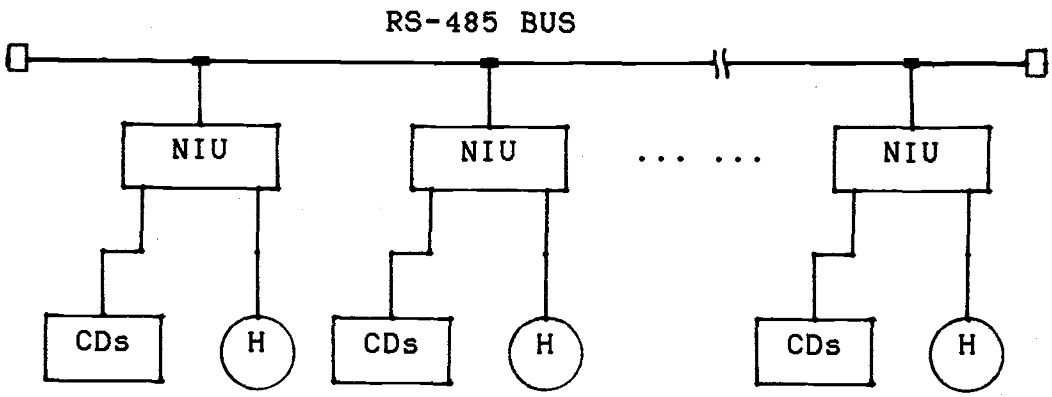


Fig.1-1 Organization of Task-Masters



CDs -- Communicating Devices

H --- Host

Fig.1-2 COLAN Organization

CHAPTER 2 LOCAL AREA NETWORKS

Local area networking has become one of the most important trends in the development of computer technology during last decade. Hundreds of research laboratories, companies, and universities have been doing a great deal of research in this area. There are many experimental LANs developed by these organizations and also many LANs are commercially available.

This chapter gives a brief description to the International Standard Organization's (ISO's) Open System Interconnection (OSI) Reference Model. Then, Ring and Bus LANs and their medium control protocols will be discussed. Here, we are only interested in the communication subnetworks, that is, the lower three layers in reference to the OSI Reference Model.

2.1 OSI Reference Model

In order to let different computers made by different companies talk to one another, the International Standard Organization has developed a set of standards which is referred as Open System Interconnection (OSI) Reference Model. The OSI Model has a hierachical structure with seven layers that define the functions involved in communicating and definitions of the services required to perform these functions. These seven layers are:

1. Physical layer
2. Data link layer

3. Network layer
4. Transport layer
5. Session layer
6. Presentation layer
7. Application layer

This Reference Model is structured as shown in Fig.2-1. The lower three layers are described briefly. For more details, refer to [TANE 81].

2.1.1 The Physical Layer

The physical layer is concerned with the electrical and mechanical characteristics of a communication channel. It defines such things as representation of a logic 1 and a logic 0 in volts; how many microseconds a bit occupies; how to initiate and terminate a connection; how many pins the network connector has and what each pin is used for. There are a number of physical medium standards for OSI communication over short distances. These include the traditional analog RS-232C, the more recent CCITT X.21, and the IEEE 802 LAN standards.

2.1.2 The Data Link Layer

In the real world, transmission of messages through an electrical medium often suffers from the disturbances of lightning, operation of electric motors, and many other noise sources. Therefore, the physical communication channel is not reliable and errors may occur during data transmission. It is up to the data link layer to make the communication channel free from errors. The physical layer merely transmits and accepts a stream of bits without any regard to the meaning or structure of the bit stream. The frame is the data communication unit in this layer. The official ISO term for frame is "physical-layer-service data unit". It is the task of the data link layer to create and recognize frame boundaries. This can be accomplished by attaching special bit patterns to the beginning and the end of the frame.

2.1.3 The Network Layer

The network layer, sometimes called the communication subnet, controls the operation of the subnet. In the network layer the unit of information is packet. Among other things, the network layer determines the chief characteristics of the Network Interface Unit (NIU), and how packets are routed within the subnet. A major design issue here is the division of labor between the NIU and the host. The network layer accepts messages from the source host, converts them to packets, and directs packets toward the destination host. Its services include network connection, data transfer, reset and connection-release functions.

In the following, we are going to discuss several LAN topologies and their relative techniques. We are only concerned with the communication subnet of these LANs, that is, the lower three layers in the OSI Reference Model. Ring and Bus networks will be discussed. A local area network can be characterized by the following factors:

(1) data rates

(2) transmission media

(3) topology

(4) channel access protocol

(5) network supervision

There are many LAN topologies. Fig.2-2 shows several. In the following, the most popular topologies ring and bus networks are to be discussed.

2.2 Ring Local Area Networks

Ring LANs have drawn enormous attention in recent years and occupy a very important position in today's LAN technology.

The data rates of most ring networks range from 1 Mbps (Mega bit per second) to 10 Mbps. These differences stem directly from the differences in the internode distances allowed by different networks, the transmission media used for the rings, and the semiconductor technologies used for constructing ring interfaces. Software overhead in distributed computing systems often limits the available data rates in a local network.

Transmission media for ring networks can be twisted wire pairs, coaxial cables and fiber-optic cables. Twisted pair is the least expensive medium for data transmission. However, it has bandwidth limitation (up to 10 Mbps for short distance) and poor noise immunity compared to coaxial cable and optical fiber. There are two basic categories of coaxial cable applications, baseband and broadband. Baseband cable can support as much as 50 Mbps. Broadband cable has much higher bandwidth (300 Mbps) and greater immunity to electromagnetic interference than baseband cable. However, some form of modulation is required for transmission, thereby increasing the cost of the node unit.

Fiber-optic cable plays an important role in local networks because of its low susceptibility to electromagnetic interfere and its very high bandwidth (over 500 Mbps). It has good security since the cable is not easily tapped. Its major disadvantages are the lack of suitable fiber-optic splicing methods and its high cost [LIU 84].

Most ring networks use unidirectional ring topologies with nodes connected in tandem via ring interfaces (single-ring topology). For the purpose of reconfiguration, some ring networks use double parallel rings (double-ring topology), with one ring used for standby operation. It is also possible for rings to be actively transmitting messages in opposite directions.

For most ring networks, all transmitters and receivers in the ring interfaces must work in synchronism at the bit level. In order to achieve this "bit synchronization", the receiver must take its timing either from a central clock via separate lines or derive timing from the line signals.

Ring network control can be separated into three levels. They are ring synchronization, channel access protocol, and network control. Network control is concerned with higher order network management functions, such as initialization of ring operation, detection and removal of lost messages, token management, reconfiguration in case of node or link failure, etc.. This level of network control is commonly called ring supervision.

The rest of this section will be devoted to the discussion of channel access protocols. There are three different protocols used in ring networks, they are token passing, empty slot and register insertion techniques. Fig.2-3 presents the ideas of these protocols.

2.2.1 Token Rings

Token ring networks are those ring networks which have the following features [TROP 81]:

* Information may flow between any pair (or greater number) of nodes rather than just to and from a central node.
* Control of the LAN is distributed among the nodes. Control is transferred from one node to another by passing a token from the former to the latter.
* Although one node may have a special responsibility for network management, it has no special privileges in normal operation.

In a token passing network, the token is a distinctive bit pattern which is passed among the nodes in a fixed sequence. A node may transmit only when it holds the token and must pass it on to the next node within a certain time.

A token passing LAN, therefore, always has a logical ring which is defined by the order in which nodes receive the token. This mechanism was originally devised for use on a physical ring (Farmer & Newhall Ring,1969) and has several advantages. The logical ring can be taken to be the physical ring, and, with unidirectional working, there is no doubt as to where the token should be passed after a node has finished with it.

All token passing networks have to deal with two key problems: lost token and duplicate token. Either may result from the failure of the physical medium or a node. Both must be remedied quickly because the loss of token means that no node can transmit, while duplication of the token generally leads to mutual jamming of the communication channel by two or more nodes. The need to deal with these conditions introduces significant complexities into what is otherwise a rather simple system. [FLIN 83].

There are many local area networks which are ring networks. These include the Newhall Ring [FARM 69], Burrough ESM Ring [PAUL80], Prime's Ringnet [GOUD 80] and IBM's Token Ring [ANDR 82] networks.

2.2.2 Empty Slotted Ring

The first proposal to use an empty slot mechanism for controlling access to a ring network was made by Pierce [PIER72]. In this scheme, individual frames of fixed length are kept circulating around the ring, marked either "full" or "empty". A node wanting to transmit a message waits until an empty slot comes by, marks it full, and begins to transmit. The frame is removed at the destination node and marked empty. This technique is called the destination removal technique. There are other ring networks using source removal technique in which the frame is removed by its source node (the sending node) instead of its destination node. This scheme differs from the token passing technique in that there may be several transmitters simultaneously putting data into empty slots rather than just one at a time.

The Pierce Ring is a destination removal empty slotted ring network. The Cambridge Ring [NEED 82] is a source removal slotted network.

2.2.3 Register Insertion Ring

One of the first proposals to use the register insertion technique for controlling access to a ring was made by Hafner, Nenadal and Tschanz [HAFN 74]. In this scheme, each interface is equipped with a shift register large enough to hold a single frame that it can be switched into the ring in series. Instead of waiting for an empty slot to pass by, a ring interface can in effect create an empty frame by switching in its buffer. The buffer is removed from the ring when the transmitted message returns to the sending node.

The Hafner ring network is a register insertion ring using the source removal technique. DLCN (Distributed Loop

Computer Network) [LIU 78] is a ring network using the destination removal technique. DDLCN (Distributed Double-Loop Computer Network) [LIU 81] and SILK (The System of Integrated Local Communications) are also register insertion ring networks.

Besides the three basic protocols described above, a number of variations and hybrid schemes for controlling access to the ring have been proposed in the literature. TORNET [VRAN 81] uses a hybrid scheme which is a combination of the empty slot and token passing protocols with source removal. This scheme is called the partial insertion slotted ring protocol. The use of this scheme can reduce message transmission delay when the ring traffic is very heavy.

2.3 BUS LANs

Bus LANs are the most popular local area networks in The United States. In a bus network, all devices (computers, peripherals, and other devices) are attached to a common communication channel, the bus, via network interface units. The major advantages of a bus network are its simplicity and low cost. It is easy to add or delete a node from the network without affecting the operation of the whole network system. The start-up and modification costs of bus networks are low compared to other types of networks.

Vulnerability to failure because of the single communication channel is the principal disadvantage of bus networks. However, the failure of a node might not cause the failure of the whole network.

Transmission media for bus networks may be twisted wire pairs or coaxial cables. Because of the difficulty in signal splitting, fiber-optics are not suitable for a bus network's communication channel. This may be considered a major disadvantage of bus networks.

Bus networks may use various numbers of unidirectional and bidirectional busses. MITRIX [MEIS 77] is a dual unidirectional bus network with one out-bound cable and one in-bound cable for receiving and transmitting. The most commonly used topology is the single bidirectional bus structure. This kind networks will be discussed in more detail in the following sections. Another topology is dual bus structure with one control bus and the other data bus [KANG81].

There are many channel access control techniques used in single bus structured networks. These techniques were classified in three major categories; selection, random access (contention) and reservation, by Luczak [LUCZ78].

Selection techniques may either be under centralized control or distributed control. There are three types of selection techniques commonly used. They are daisy-chaining, polling, and independent requests.

Random access, or contention, techniques are characterized by a lack of strict ordering of the nodes contending for access to the communication channel. In a contention network, a node is free to broadcast its messages. When a node has a message it starts transmission without regarding to whether there is other transmission. In CSMA technique, a node starts to transmit immediately when it senses that there is no transmission going on.

Reservation techniques include time-slotted, polling, daisy-chaining and token passing. In the time-slotted technique, the communication channel is shared among nodes of a network by allocating to each one a time slot during which only they can transmit messages. As another way, the network controller may poll each device in the network to determine if it has messages to transmit. In daisy-chaining network, the control of the network is passed from one node to the next, either by the same transmission medium or by a separate circuit. Token passing is a kind of daisy-chaining technique in which the control of the network is passed from one node to another by passing a control token (the same as in the cases of token ring).

In the following, contention and reservation techniques are discussed with the emphases on CSMA/CD (Carrier Sense Multiple Access with Collision Detection) technique (contention) and token-passing technique(reservation).

2.3.1 CSMA/CD Technique

The first random access protocol, known as the pure ALOHA [ABRA 70] technique, was used in the ALOHA system at the University of Hawaii. In the pure ALOHA technique, a node can transmit its messages at any time without determining if there is any other node transmitting. The transmission may succeed or fail depending on if there is more than one node transmitting in an overlapped time period. If two or more nodes simultaneously transmit messages, there is a collision and the transmission fails. The peak throughput for pure ALOHA is only 1/2e (or 0.18).

In slotted ALOHA, a restriction is added to the pure ALOHA system. Now, a node may start transmitting only at the beginning of a fixed time slot sequence. The peak throughput of slotted ALOHA system is 1/e (0.36), double that of the pure ALOHA system.

In ALOHA systems, a node may transmit its messages even if there is another node transmitting. This can cause a great many collisions. The ALOHA technique may be modified so that a node wishing to transmit its messages first listens to the communication channel to determine if there is transmission in progress. If there is no transmission, it starts transmission. Otherwise, it waits till the transmission is finished then starts transmission. This can avoid many collisions and therefore improve the throughput of the system greatly. CSMA (Carrier Sense Multiple Access) was developed by following this idea.

In the CSMA technique, a node wishing to transmit first listens to the channel to determine if another transmission is in progress. If the channel is idle, the node may transmit. Otherwise, the node backs off some period of time and tries again, using either non-persistent, 1-persistent, or p-persistent algorithms.

In non-persistent CSMA technique, a node wishing to transmit listens to the channel and obeys the following rules[STAL 84]:

1. If the channel is idle, transmit

2. If the channel is busy, wait an amount of time drawn from a probability distribution (the retransmission delay) and repeat step 1.

To avoid channel idle time, the 1-persistent protocol can be used. A node wishing to transmit listens to the channel and obeys the following rules:

1. If the channel is idle, transmit
2. If the channel is busy, continue to listen until the channel is sensed idle, then transmit immediately

3. If there is a collision (determined by a lack of acknowledgment), wait for a random amount of time and repeat step 1.

Whereas non-persistent nodes are deferential, 1-persistent nodes are selfish. If two or more nodes are waiting to transmit, a collision is guaranteed. A compromise that attempts to reduce collision, like non-persistent, and reduce idle time, like 1- persistent, is p-persistent. In the p-persistent algorithm, a node wishing to transmit listens to the channel and obeys the following rules:

1. If the channel is idle, transmit with probability p, and delay one time unit with probability (1-p). The time unit is typically equal to the maximum propagation delay of the whole channel

2. If the channel is busy, continue to listen until it is idle and repeat step 1

3. If transmission is delayed one time unit,repeat step 1.

The maximum utilization achievable using the CSMA technique can far exceed the pure and slotted ALOHA techniques. The maximum utilization depends on the length of the frame and the propagation time. The longer the frame or the shorter the propagation time, the higher the utilization.

CSMA, although more efficient than ALOHA techniques, still has one glaring inefficiency. When two or more nodes starts transmitting at the same time and collision occurs, the channel remains unusable for the duration of transmission of the damaged frames. For long frames, compared to propagation time, the amount of wasted bandwidth can be considerable. This waste can be reduced if a node continues to listen to the channel while it is transmitting and stops transmitting immediately if a collision is detected. In this case, these rules can be added to the CSMA rules:

1. If a collision is detected during transmission, immediately cease transmitting the frame, and transmit a brief jamming signal to assure that all nodes know that there has been a collision

2. After transmitting the jamming signal, wait a random amount of time, then attempt to transmit again using CSMA.

This protocol is called CSMA/CD (Carrier Sense Multiple Access with Collision Detection). The most commonly selected algorithm for CSMA/CD is 1-persistent. The 1-persistent algorithm, i.e., for p=1, would seem to be more unstable than p-persistent due to the greed of the nodes. What saves the day is that the wasted time due to collision is normally short if frames are long relative to propagation delay. With random backoff, the two nodes involved in a collision are unlikely to collide on their next tries. To ensure that backoff maintains stability, Ethernet uses a technique known as binary exponential backoff. A node will attempt to transmit in the face of repeated collisions. After each collision, the mean value of the random delay is doubled. If a node fails to transmit for 16 times, it will assume that there is a failure in the system and it stops trying.

The beauty of the 1-persistent with exponential backoff is that it is effective over a wide range of loads. At low loads, 1-persistent guarantees that a node can seize the channel as soon as it goes idle, in contrast to the non- and p-persistent schemes. At high loads, it is at least as stable as the other techniques. However, one unfortunate effect of the Ethernet backoff algorithm is that it has a last-in, first-out effect; nodes with no or few collision will have a chance to transmit before nodes which have waited longer.

2.3.2 Token Bus

Token bus is a relatively new technique for controlling access to a broadcast medium, inspired by the token ring technique. The token bus technique is more complex than CSMA/CD. For this technique, the nodes on the bus form a logical ring. The nodes are assigned logical positions in an ordered sequence with the last member of the sequence followed by the first. Each node knows the identity of the nodes preceding and following it. The physical ordering of the nodes on the bus is irrelevant and independent of the logical ordering.

As in the token ring networks, the token is a specific bit pattern. A node which possesses the token is granted control of the medium for a specific time. The node may transmit one or more frames and may poll nodes and receive responses. When the node is done, or the time is expired, it passes the token on to the next node in logical sequence. This node now has the permission to transmit. Hence steady-state operation consists of alternating data and token transfer phases. Non-token nodes can only respond to polls or requests for acknowledgment.

The token bus scheme requires considerable maintenance. The following functions, at a minimum, must be performed by one or more nodes on the bus:

* Ring initialization: When the network is started up, or after the logical ring has broken down, it must be initialized. Some cooperative, decentralized algorithm is needed to sort out who goes first, who goes second, and so on.

* Addition to the ring: Periodically, non-participating nodes must be granted the opportunity to insert themselves in to the ring.

* Deleting from the ring: A node must be able to remove itself from the ring by splicing together its predecessor and successor.

* Recovery: A number of errors can occur. These include duplicate address (two or more nodes think it is their turn and therefore multi-token) and broken ring (no node thinks it is its turn, lost token).

There have been several token bus standards, IEEE 802 Token Bus and Manufacturing Automation Protocol (MAP) which was developed by General Motor for programmable devices to communicate in the factory environments [KAMI86].

2.4 CSMA/CD versus Token Bus

At present, CSMA/CD and token bus are the two principal contenders for medium access control techniques on bus topologies [STAL84]. Table 2-1 attempts to summarize the advantages and disadvantages of these two techniques.

As mentioned before, development of token bus technique was inspired by the token ring technique. Therefore, token bus and token ring have many similarities. So, we can compare token bus technique with CSMA/CD technique indirectly by comparing token ring and CSMA/CD. Bux [BUX 81] made a performance comparison among several LAN techniques. These techniques are token ring; slotted ring (empty-slot technique); CSMA/CD; and MLMA (Multi- Level Multiple-Access) bus. We are interested in token ring and CSMA/CD bus only. The delay-throughput relation of token ring and CSMA/CD bus for two data rates, 1 Mbps and 10 Mbps, is shown in Fig.2-4 [KUMM 82].

TABLE 2-1 CSMA/CD vs. Token Bus [STAL84]

advantages	disadvantages
CSMA/CD	
Simple algorithm	Collision detection requirement
Widely used	Fault diagnosis problems
Fair access	Minimum packet size
Good performance at low to medium load	Poor performance under very heavy load
	Biased to long transmission
Token Bus	
Excellent throughput performance	Complex algorithm
Tolerate large dynamic range	Unproven technique
Regulated access	

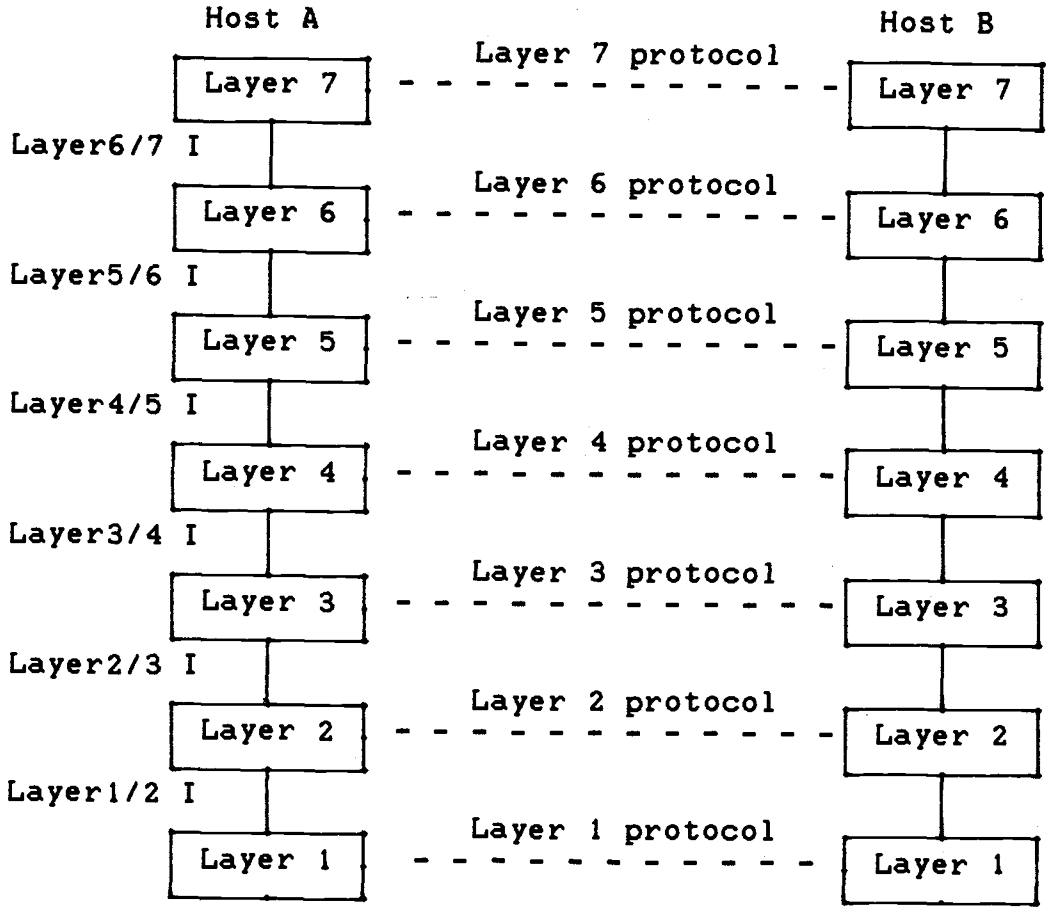


Fig.2-1. OSI Reference Model

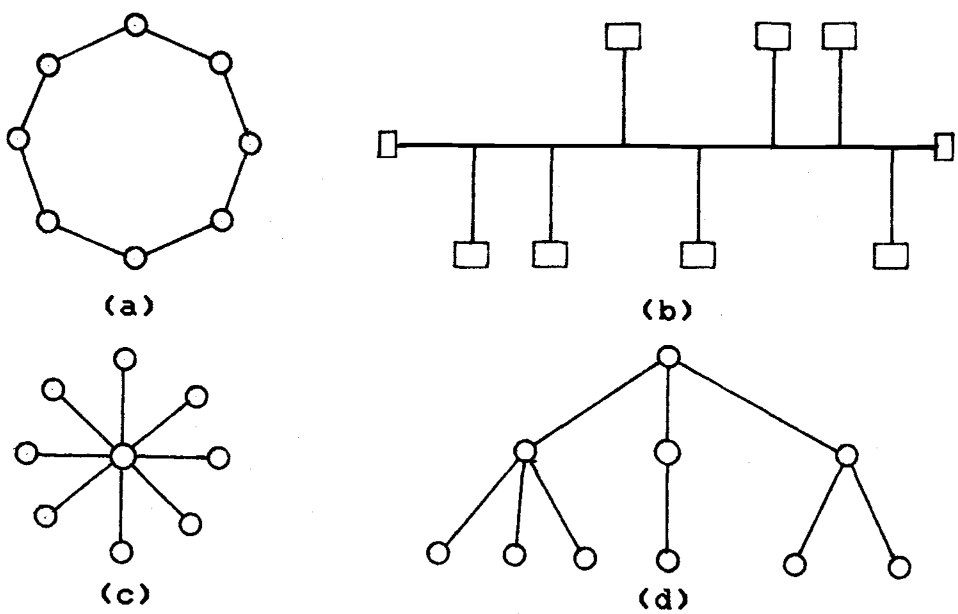
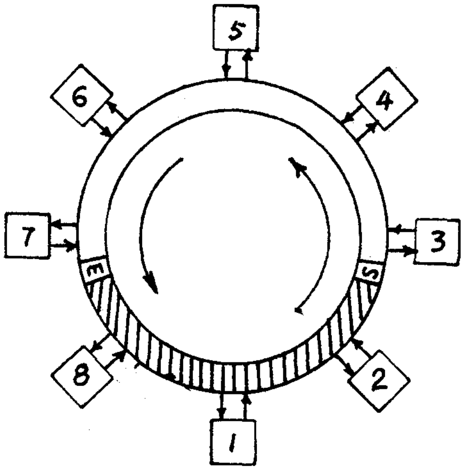
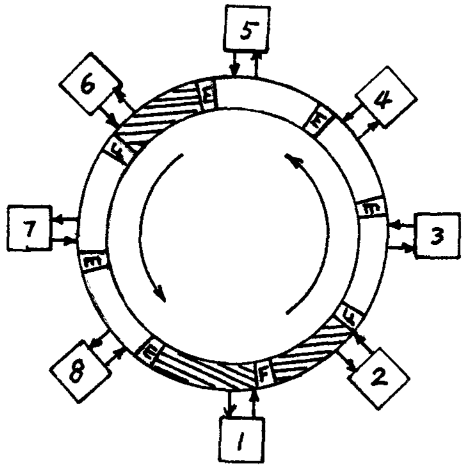


Fig.2-2. Some popular topologies. (a) Ring. (b) Bus. (c) Star. (d) Tree



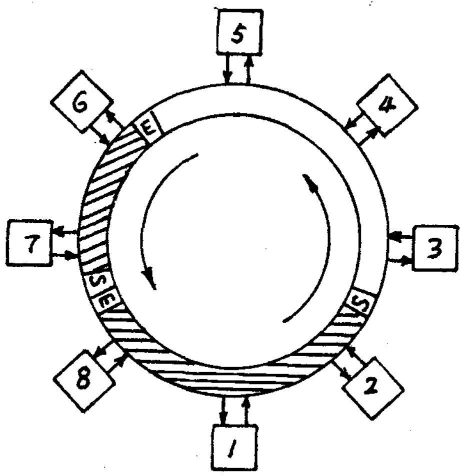
S: Start of Message
E: End of Message

(a) Token Ring



F: Full
E: Empty

(b) Empty Slot



S: Start of Message
E: End of Message

(c) Register Insertion

Fig.2-3. Three ring net control techniques

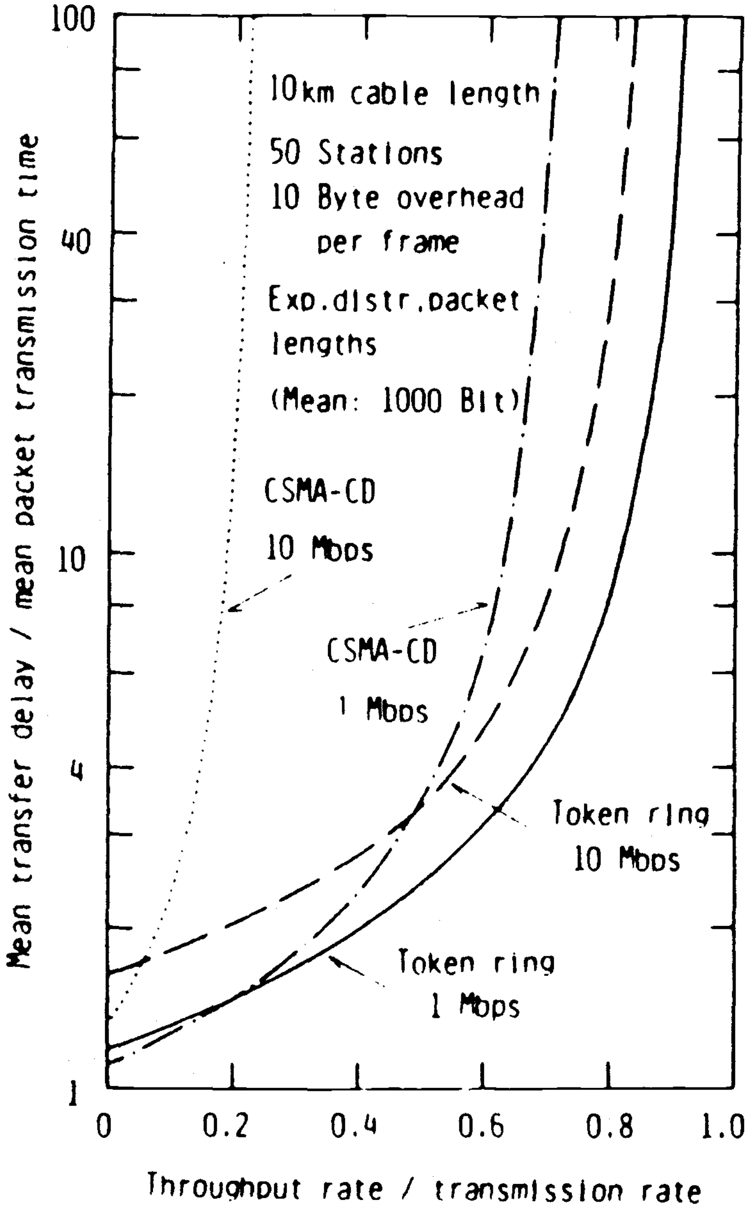


Fig.2-4. Delay-Throughput Characteristic for Token Ring and CSMA/CD Bus [KUMM 82]

CHAPTER 3 COLAN ARCHITECTURE

COLAN (Control Oriented Local Area Network) is designed to improve the performance of the Task-Master as an NIU (Network Interface Unit). This chapter addresses the design of the COLAN architecture, its switching mechanism, and its channel access control mechanism.

3.1 Overview

COLAN will adopt a single bus topology. Packet switching technique is employed for communication among the nodes of COLAN. The outstanding characteristic of COLAN is that it employs a hybrid channel access control protocol for the channel control. This hybrid protocol combines the CSMA/CD technique and the token bus technique.

COLAN has two network operating states and four nodal operating modes. They are Non-Token State, Token State, Local Mode, Network Requesting Mode, Network Mode, and Control Passing Mode. Communication among different nodes of the network is allowed only when the network is in the Token State. If no transmission is required, the network is in Non-Token State. When any node requests for access to the communication channel, COLAN employs the CSMA/CD technique to generate a control token. When the token is generated, the node can start transfer. This node is allowed to access to the channel for a limited amount of time. When the time expires, the node must pass the control token to another node. The other node now can start transmission. If a node finishes its transmission and there is no another node wishing to use the channel, the node will destroy the control token and the network will work in Non-Token State. If again, any node wishing to communicate, the CSMA/CD technique is again employed to generate a token.

To implement this hybrid protocol, five timers are needed. They are T1, T2, T3, T4, and T5. T1 is used by the CSMA/CD technique to determine whether the communication channel is busy. T2 is used by the network to recover from a lost token error when the network is in Token State. T3 is used by the token technique. A node must wait till its T3 times out before it claims the hold of the token. T4 is employed by CSMA/CD technique for collision detection. And T5 is the time period for a node to hold the control token.

3.2 Subnetwork Architecture

Low cost and simplicity are emphasized in the design of COLAN. The following design activities will constantly present these concerns.

3.2.1 Bus topology

A bus topology was selected for COLAN. Bus LANs have the advantages of simplicity and low cost start-up and modification compared to other types of networks.

COLAN has a single common communication channel which meets EIA RS-485 standards. Its configuration is shown in Fig.3-1. Communicating devices are connected to the bus via

NIUs. Each node of the network consists of an NIU and other communicating devices attached to the NIU. Because of the limited driving ability of the RS-485 transmitter adopted, COLAN may have up to 32 nodes without any other transmission mechanism. If more than 32 nodes are required for the network, repeaters (or bridges) are needed to connect two or more sections together. A further limitation comes from the fact that an NIU in COLAN uses a 6-bit switch as its address mechanism and therefore the addressing ability ranges from 0 to 63. Address 0 is reserved for use as a broadcasting address (every node recognizes this address as its own address). further expansion may be done by adding new address switches to each NIU and this can be done without difficulty. Virtually, COLAN may have as many nodes as required.

3.2.2 The communication channel

In COLAN, twisted wire pair is employed as the communication medium. Again, this is because of the low cost and simplicity properties of twisted pair. The length of the bus may range up to 1.2 km (or 4000 feet) without any repeater. It operates from a single 5- volt power supply. Fig.3-2 shows the interface of the NIU to the Bus. When the voltage difference of wire A and wire B is greater than or equal to 0.2 volt, i.e., A-B>=0.2V, it represents a logic 1. When A-B<=0.2V, it represents a logic 0.

The 8051 microcomputer's on chip serial communication port (UART) in the NIU is used for transmitting and receiving messages to and from the bus. An asynchronous communication technique is employed and transmission rates ranging from 122 bps to 31,250 bps (bit per second) are possible. This baud rate limitation comes from the 8051's UART.

There is no hardware facility for error detection during data communication within the MCS-51. Therefore software facilities must be provided to make the channel reliable. A CRC (Cyclic Redundant Code) code is generated at the source node and is also transmitted to the destination node with the data in a packet. The destination node generates a CRC code from the data received, and compares this CRC code to the one received. If both CRC codes are the same, the destination node sends an acknowledgment to the source node. Otherwise, it sends a negative acknowledgment to notify the source node that errors have occurred and retransmission is needed.

3.3 Switching Mechanism

A packet switching technique is employed in COLAN. The external data memory of an NIU is divided into three sections. One section is used as transmitter buffer, another is used as receiver buffer, and the third is used for other purposes, such as a command queue.

When a node possesses the control token it may transmit messages to other nodes of the network for a certain amount of time. These messages are in the form of packets. There are two types of packets, Network Packets and Local Packets. The Network Packets are intended for communication among the nodes of the network. The Local Packets are used for communication between the NIU, the Host, and other nodal resources. The formats of these packets are defined in Chapter 4. When the time for the node to access the channel expires and one or more complete packets have been transmitted, the node has to pass the control to another node. If the node has more messages to transfer, it stores them in the transmitter buffer and waits until it regains the control token again before continuing its transmission.

The transmitter buffer is used to store packets when a node is waiting for access to the communication channel. At the destination node, incoming packets are stored in the receiver buffer.

3.4 Control Mechanism

In COLAN, there are two network operating states and four nodal operating modes. These two states are Non-Token State and Token State. The four nodal modes are Local Mode, Network Mode, Network Requesting Mode, and Control Passing Mode. Fig.3-3 shows the transformation of the two states and the transformation of the four modes. There is a TOKEN State Flag in each NIU to record if the network is in Token State. If it is set, the network is in Token State. Otherwise, it is in Non-Token State. There are two flags in each NIU to present the four nodal modes. One is NR Flag. When the node wishes to communicate it first sets this flag. The other is Network Flag. When a node holds the token it is set. The definitions for Non-Token and Token States are given below:

Non-Token State: In this state, there is no control token in the network and therefore there is no transmission among any pair of nodes allowed. When COLAN powers up, it enters this state and stays in this state until a token is generated. The generation of the control token transforms the network to the Token State. COLAN returns to the Non-Token State when the token is destroyed purposefully or by accident. When there is no node wishing to transmit data, the system destroys the the token and the network enters the Non-Token State. This is done to improve operating efficiency.

Token State: When any node in the network possesses the control token, the network is in Token State. Communication among nodes is possible only in this state.

The operating modes are defined as below:

L MODE: Local Mode. In this mode, the resources of a node (both hardware and software) are accessible to any device of the node, specially to the host device. The network resources of other nodes are not accessible to this node. Data may flow inside the node (among its devices) or data may flow into this node from the network. No data may flow out to the network.

NR MODE: Network Requesting Mode. When a node wishes to transmit messages to other nodes of the network it must first enter the NR MODE from L MODE by setting a NR Flag. Then it checks its TOKEN Flag. If it is set, it waits for the token to pass by and "catches" the token (the network is in the Token State). It then starts transmission. If, however, the network is in Non-Token State, it would try to generate a control token. If it succeeds in generating the token it starts transmission. If another node succeeds in generating the token, this node will set its TOKEN Flag to indicate the network is in the Token State now and wait for the token.

N MODE: Network Mode. A node will enter the N MODE from NR MODE if it catches the control token (if the network is in Token State) or if it has succeeded in generating the token (if the network was in Non-Token State). In this mode, the node can transmit data in the form of packets to any other node (or nodes) of the network. The Network Flag is set when a node enters this mode.

CP MODE: Control Passing Mode. When a node finishes its data transmission or when the time for the node to access the channel has expired, the node must pass the control token to another node. If the node has finished its transmission, it resets its NR Flag and broadcasts a token passing packet and waits for another node to capture the token. If there is no other node wishing to transmit data and therefore no node claims the token, this node will broadcast a token destroyed packet to inform all other nodes to enter the Non-Token State and then destroys the token. The network is now in the Non-Token state and the node is in the L MODE. If there is a node claiming the token, the node will reset its Network Flag and enter its L MODE. If the node has not finished transmission but the time has expired, it would pass the token to other node and wait until its next turn for the token to pass by. If there is no other node wishing to transmit, the node can still hold the token for another time period and continue its data transmission.

COLAN employs a hybrid channel access control technique which combines the token bus technique and a CSMA/CD like technique. When the load of the network is light, COLAN operates like a CSMA/CD bus network. This is done by purposefully destroying the token. COLAN determines the utilization of the communication channel by monitoring token capture by other node. If no other node takes the token after a node finishes its transmission, it assumes that the network load is light. When the load is light, the network destroys the token and works like a CSMA/CD bus network. This corresponds to the Non-Token State. If any node wants to transfer, it has to contend for generating a token first. Because the load of the network is light, the process of generating the token is likely to be successful most of the time. In this case, the time for generating the token is much shorter than waiting for the token to pass by. For an N node network, the average time to wait for the token to pass by is T*(N/2), where T is the unit time used in token passing process and is defined later. This means that a node would wait N/2 times longer if using token passing. (The process for generating the token and the process for passing the token take about the same time, if there is no collision.)

As the load of the network grows, the number of collisions increases. This makes a token passing technique advantageous to CSMA/CD technique when the load is heavy.

In COLAN, if the load of the network is heavy, the network would work in Token State. This will be very fair to each node and also has a higher throughput. The delay-throughput characteristics of token ring and CSMA/CD bus are shown in Fig.2-4.

When the network powers up, all nodes enter the L MODE. The network does not have a token (in Non-Token State) until one or more nodes wish to transfer and generate a token. In COLAN, no particular node is responsible for generating the token. If the network is in Non-Token State, each node would try to generate the token when it wishes to communicate. Five timers are needed in this hybrid protocol. These timers are described below:

T1 is a delay timer which is used to determine whether there is communication in progress on the channel. When the network works in the Token State and a node has just powered up and wishes to transmit,it must delay and listen to the channel for the T1 time period to prevent the node from interferring with the transmission of another node. T1 must be large enough to allow the node to determine whether there is a transmission in progress.

T2 is used by the network to recover from a lost token failure. When the network is in the Token State, if a node wishing to transmit has not heard a transmission on the channel for all the period of T2, it will consider that the token has been lost and will try to generate a new token. Lost token may result from the failure of a node, or transmission errors which changes the token passing packet into an invalid one.

T3 is the time for a node to delay to claim the holding of the token. Assume that COLAN has N nodes and their addresses are from 1 to N, with address 0 used as the broadcasting address. Also assume that the current token holder's address is n, and my address is m. Then T3 can be determined according to the following formula:

$$T3 = D*T = \begin{cases} (m-n)*T & ; \text{ for } m>n \\ (N+m-n)*T & ; \text{ for } m<n \end{cases}$$

where T is a time unit which is large enough to prevent node (m+1) from claiming the token before node m has finished the claim if node m wishes to transmit. The node immediately following the present token holder has the least T3 value and therefore its T3 would be the first one that times out if it wishes to communicate. If there is another node betweeen the present token holder and node m (in logical order) wishing to communicate, node m can not claim the token because its T3 is greater than that node's. Therefore, only if there is no another node between node m and the present token holder, can node m claim the capture of the token.

During the token generation period, there may be more than one node contending for generating the token. Therefore a collision is possible. When a node determines that there is no token in the network and it wants to generate a new token, it broadcasts a token generating packet. If two or more nodes try to generate the token at the same time, a collision occurs and a node may not be able to receive anything from the channel because the receiver may have been jammed. T4 is employed to prevent a receiver from being jammed forever. After broadcasting the token generating packet, if a node still has not received a complete packet from the channel when T4 times out, it determines that the receiver has been jammed. Then the node will delay a random amount of time and try to generate the token again.

Timer T5 is the time period for a node to hold the control token. When T5 expires, the node has to pass the token to another node if there is any node wishing to claim it.

When the network is in the Non-Token State, each node wishing to communicate obeys the following rules:

1. The NIU sets its NR Flag and checks its TOKEN Flag to see if the network is in the Token State. If the Flag is set, it is in the Token State, start T2 and wait for the token to pass by. Otherwise, the network is in the Non-Token State, go on to step 2.
2. Start T1 and listen to the channel until either hear the transmission in the channel or T1 times out.
3. If hear transmission on the channel, stop T1 and set the TOKEN Flag, then start T2 and wait for the

token. If T1 times out, go on to step 4.

4. Broadcast a token generating packet and at the same time try to receive the packet. Start T4, go on to step 5.
5. If the packet has been received, compare it to the one transmitted. If they are the same, set TOKEN Flag and Network Flag, start communication. If they are different, delay a random amount of time then go back to step 2. If until T4 times out it still has not received the packet, it assumes that a collision happens, go back to step 2.

In the Token State, if a node wants to transmit messages, it must first capture the token. The process for a node to determine its turn for access to the channel is determined by the following rules. Each node wishing to communicate obeys the following rules:

1. When a token passing packet has been received, check the NR Flag, if it is set, calculate T3 and start timer T3. Otherwise, ignore the packet.
2. If a token claiming packet is received before T3 times out, stop T3 and wait for the next token.
3. If T3 times out, claim the token by broadcasting a token claiming packet. Set its Network Flag, then start data transmission.

When the time for a node to keep the control token has expired, the node has to pass the control to another node. The timer T3 of a token holder is selected so that $T3 >= N*T$.

The process for passing the token to another node is carried out by the following rules:

1. Broadcast a token passing packet and start the T3 timer.
2. If a token claiming packet is received, stop T3 and clear the Network Flag.
3. If T3 times out, check if there is any more data in the transmitter buffer or NR Flag is on. If yes, set the Network Flag and continue the transmission. Otherwise, no packet is in the transmitter buffer and the NR Flag is cleared, broadcast a token destroying packet to inform other nodes to enter the Non-Token State and then destroy the token by clear the Network Flag and the Token Flag.

After the token is destroyed the network is in the Non-Token State. If any node wants to transfer data, the process of token generation and token passing begins again.

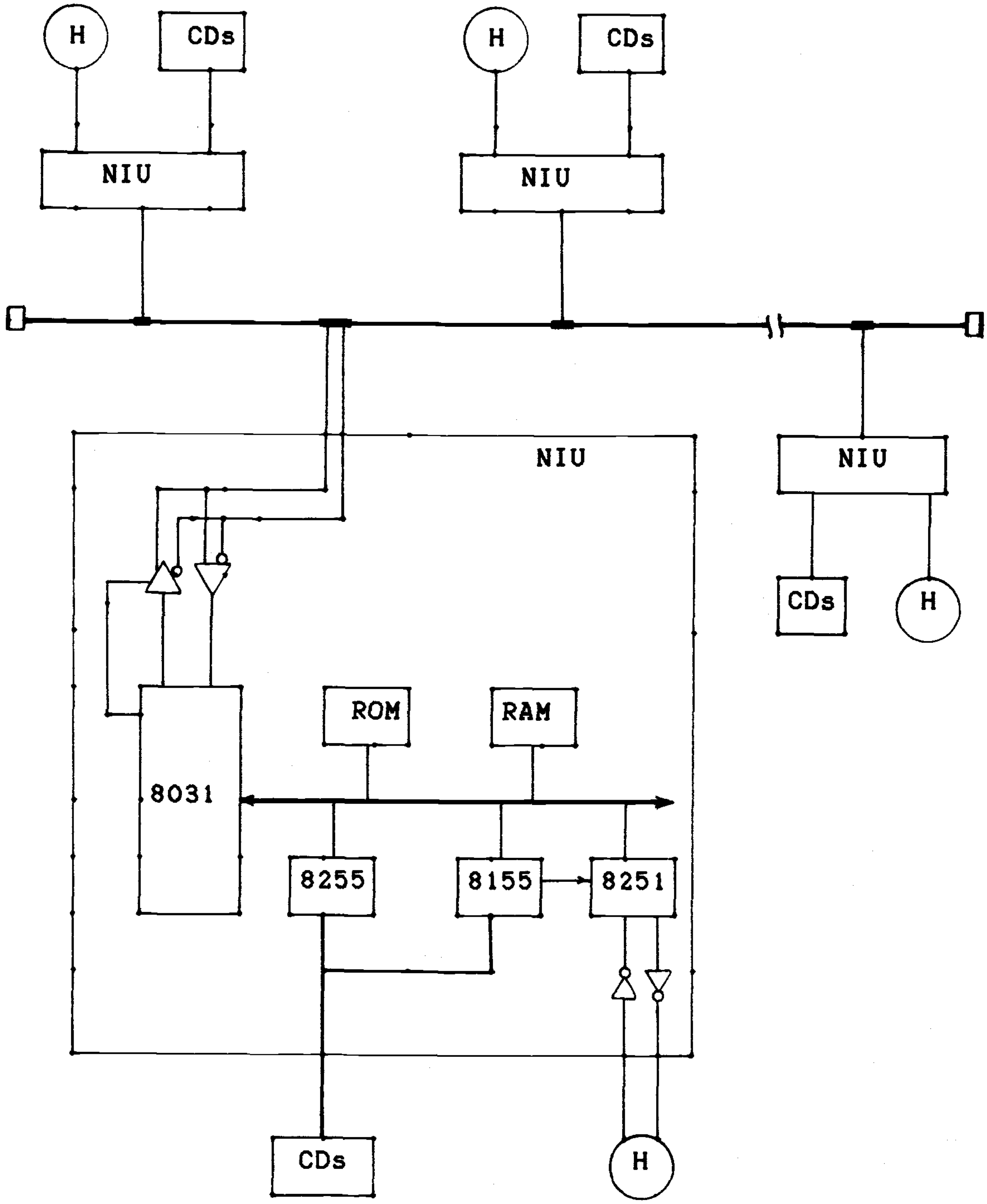


Fig.3-1. COLAN Architecture

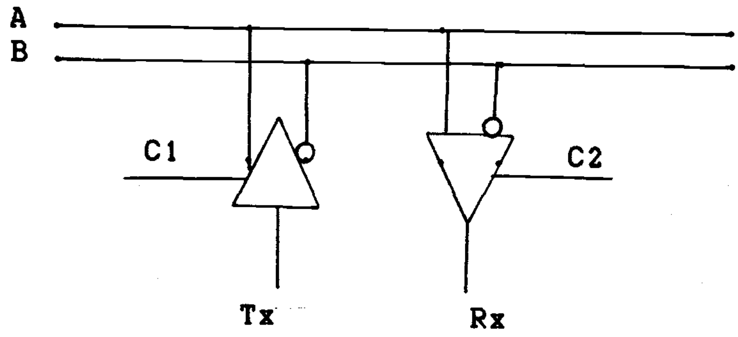
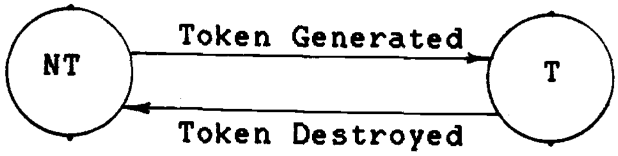
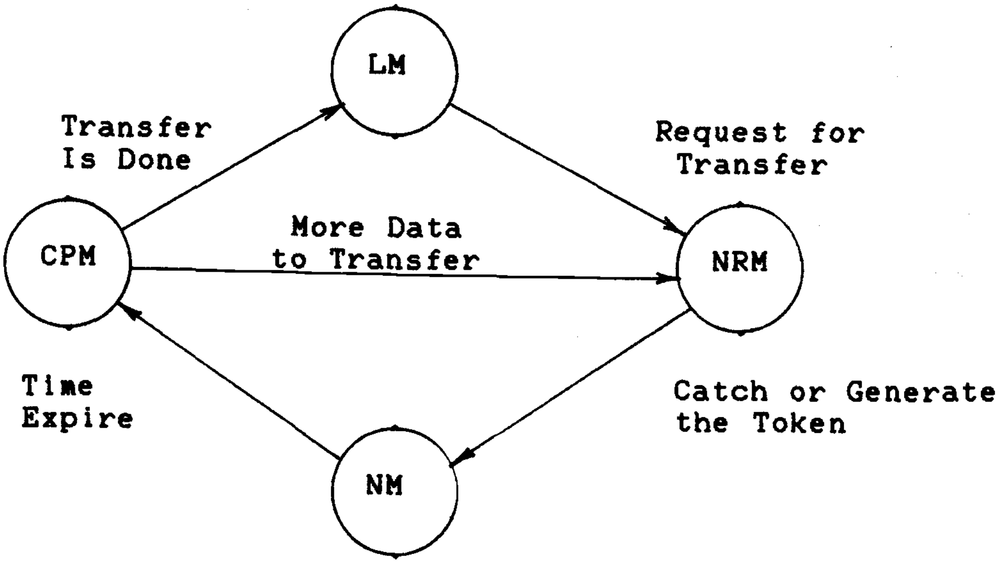


Fig.3-2. Transmitter and Receiver Configuration



(a)



(b)

Fig.3-3. Transform Diagrams (a) States (b) Modes

CHAPTER 4 COLAN DESIGN

Chapter 3 considered the network architecture, the communication channel, the information switching mechanism, and the network control mechanism. This chapter presents the the design of the mechanisms for token generation, token passing, and token destroying. The packet formats are discussed in the second section. The last section discusses the design of the network interface unit.

4.1 Network Control

This section is devoted to the discussion of the design of the control mechanism of the COLAN. The State Diagram, the Token Generating Flow Chart, Token Passing Flow Chart, and Token Destroying Flow Chart will be presented.

4.1.1 Control State Diagram

The control of the network is equally distributed among all nodes of COLAN and no single node has the special responsibility for supervising the operation of the network. The operation of each node may be presented by its state diagram given in Fig.4-1.

In the diagram, the notations are defined as below:

RT: Request for Transfer. When a node works in its L MODE and wishes to transmit messages, its host must send a channel access request to its NIU before the node can access to the channel. When RT is received, the NIU will set its NR Flag.

TX: Transmission is in progress. This implies that the channel is busy and the network is in the Token State.

NTX: No Transmission on the channel. The channel is idle and the network is in Non-Token State. The node may try to generate a token.

F: Fail in trying to generate a token. This happens when a node tries to claim a new token and a collision occurs.

S: Success in generating a new token. The node has successfully claimed the new token and it becomes the current token holder. The network transforms from Non-Token State to Token State.

TP: Token has been Passed to another node.

TC: Token has been Caught by this node.

TD: Token is Destroyed. Network transforms from Token State to Non-Token State.

The operations of a node in each state are as followings:

S1: State 1. When a node powers up or after the control token is destroyed, a node works in S1. In S1, all of the resources of this node are accessible to its host but no other network resources are available. This corresponds to the case that the network is in Non-Token State and the node is in L MODE.

S2: From S1, when a node requests access to the channel it enters S2. In S2, the Network Request

Flag is set and the node listens to the channel. It corresponds to Non-Token State and NR MODE.

S3: When a node has not heard transmission on the channel for the T1 time period, it tries to generate a control token. It broadcasts a token generating packet to the network and receives the packet at the same time. If no collision occurs, it will receive the packet correctly and become the token holder. Transmission may follow immediately and the network enters the Token State. If it fails to receive the token completely and correctly, it goes back to S2 and tries the process again. S3 also corresponds to Non-Token State and NR MODE.

S4: The network is in the Token State and the node is in the N MODE. A node enters this state either from S3 (it has succeeded in generating a token) or S6 (it has succeeded in acquiring the token). In this state, a node can access the communication channel for a certain amount of time (T5). When the time expires, it has to pass the control to another node, then it may go to S5 or S6.

S5: From S1, if a node hears transmission on the channel, it determines that the network is in the Token State and sets its own token flag to indicate that. By setting the flag, the node transforms from S1 to S5. When a node has finished its transmission and has passed the control, it also enters S5 from S4. In S5, the host of a node may use the resources of this node but no other resources of the network. If there is no node taking the token over, the node will destroy the token and it will enter S1 and the network enters Non-Token State.

S6: When the time for a node to keep the token has expired the node has to pass the control to another node. If it has more messages to transmit, it enters S6 from S4. In S6, the NIU of a node may receive data from its host or other devices and store them in its transmitter buffer, and waits to acquire the token again. When this happens it continues its transmission.

4.1.2 Token Generation

When COLAN is in Non-Token State and there are one or more nodes wishing to transmit, the network must enter the Token State and therefore a control token must first be generated. The generation of the token is the result of a successful contention among the nodes wishing to transmit. In generating the token, a CSMA/CD like technique is employed. The process of generating the token can be presented by a flow chart and is shown in Fig.4-2.

In the flow chart, some symbols are defined as below:

Token: Represented by a token flag, when it is set, the network is in the Token State.

PR,PT: Packet Received and Packet Transmitted. If PR=PT the node succeeds in generating the token and becomes the token holder, otherwise, it fails in generating the token and may try again.

The timers, T1 and T4 are the same as defined in chapter 3.

4.1.3 Token Passing

The control access to the communication channel is passed from one node to another in a logical ring by passing the control token. A node which possesses the token, referred as the token holder, is allowed to transmit data for a limited time. When the time expires it must pass the token to another node if there are other nodes waiting for access to the channel. If, however, there are no other nodes waiting for the control token, it can hold the token for another period of time.

The process for a token holder to pass the control token to another node is shown in the flow chart in Fig.4-3. It is assumed that the network has N nodes and their addresses are from 1 to N. T3 is the delay timer whose value is the time that a node has to wait before it can claim the token. T5 is the time for a node to hold the token.

When COLAN is in the Token State, a node wishing to transmit must capture the token before it is allowed to access the channel. This process is depicted by Fig.4-4. In the flow chart, the symbols are defined as follows:

m: m is the address of a node which is waiting for the token, or simply my address

n: the address of the present token holder. n is passed to other nodes in the token passing packet.

N: as defined previously, N is the number of nodes in COLAN.

All other symbols are the same as defined in chapter 3.

4.1.4 Destroying the Token

In COLAN, when there is no node wishing to transmit, the control token is destroyed rather than continuously circulating it among the nodes. When a token holder finishes its data transmission, it tries to pass the token to another node. If there is no node claiming the token, the token holder broadcasts a Token Destroyed packet to inform all nodes to enter the Non-Token State. Then it clears its own Token Flag and Network Flag; these destroy the token. This process is depicted by Fig.4-3 and Fig.4-5.

4.2 Data Link

Communications in COLAN is performed by exchanging packets among nodes. This section defines the packet formats for inter and intra node communications, i.e., among the nodes and between a host and its NIU.

When communicating between nodes, it is essential to know the packet destination, the packet source, the functions to be performed, the messages, and, finally, whether the transmission has been carried out correctly. According to these requirements, the packet format is defined as follows:

F (8)	DA (8)	SA (8)	TN (8)	DATA (variable)	CRC (16)	F (8)

F Field: Flag field, this is used to denote the beginning and the end of a packet. In COLAN, the special characters "{" and "}" are used to denote the beginning and the end of a packet.

ADDR. : DA and SA are address fields standing for Destination Address and Source Address respectively. Though addresses are 6-bit each, 8-bit bytes are transferred because of the properties of asynchronous transmission

TN Field: Task Number field. In COLAN, control operations are performed in the form of tasks. The task number is actually the control message which tells the destination node how to process the data.

Data: Data field contains messages to be sent to the destination node, to its host, its printer, or other devices. It may contain parameters needed for the destination node to execute the task.

CRC Field: Check character field. This field is for the purpose of detecting transmission errors in a packet.

When a node is in the L MODE, data may be exchanged among its devices, such as host to NIU, host to printer, and so on. Under this condition, destination node and source node are implied and are no longer needed. The Checksum field may also not be needed. Therefore, the packet format for communication inside a node is defined as below:

F (8)	TN (8)	DATA (variable)	F (8)

Each field stands for the same meaning as before.

As mentioned before, an asynchronous communication technique is employed and its transmission unit is a data byte. Normally a 10 bit frame is used. In practice, a data byte is transmitted from one node to another in an 11-bit frame as shown below (this data format is a specific feature of the MCS-51 microcomputer chips):

START	8-bit DATA	ADDR/DATA	STOP

START: Start the transmission of a frame. This notifies the receiver to start receiving a data byte.

8-bit DATA: Data field contains the data byte.

ADDR/DATA: This is the nineth bit of a received character in the nine-bit character mode. This is a specific feature offered by the MCS-51 microcomputer. When the data field contains the beginning flag "{" or an address byte, this bit is set to "1". A "1" in this bit wakes up all the nodes, that is, all nodes will respond to the character. When it is "0", the unrelated nodes do not respond to the data transmission. For data characters this bit is set to "0".

STOP: Stop the transmission. It tells the receiver that a complete frame has been transmitted and to stop receive data. The Start turns the channel into busy and Stop changes it back to idle.

4.3 Network Interface Unit Design

All the communicating devices in COLAN share a single common communication channel, and therefore a control mechanism must be provided for the devices to share the channel. The Network Interface Units provide these control functions. According to the properties of the NIU, a microcomputer is selected as the NIU controller. Remember that COLAN is a control oriented LAN, The NIUs are not merely interfaces connecting devices to the channel, they are also equipment controllers which control the operations of the devices connected to the nodes.

Each NIU is an intelligent bus interfacing unit and an equipment controller. It has a responsibility to share the network supervision burden, such as collision detection, token generation, token passing, etc.. It also must participate in controlling a device's operation. A conceptual NIU configuration is shown in Fig.4-6. The basic functions which must be carried out by an NIU can be sorted into three types:

1. network-oriented functions
2. host-oriented functions
3. device-oriented functions

These functions are discussed in the following.

4.3.1 Network Oriented Functions

Network oriented functions are concerned with the operations of network supervision and the control of the information transmission among nodes. The following five basic tasks must be carried out by the network oriented part:

a. Collision detections
b. Control of the token
c. Control of message transmission
d. Control of message reception
e. Address recognition

The five tasks above are all related to the network serial communication port, and they are performed by the micro-computer. The collision detection function is employed during the token generating period.

4.3.2 Host Oriented Functions

A host device is connected to the network via a NIU. The host is connected to the NIU through a RS-232C channel. The host oriented part of the NIU handles the message exchange between the host and the NIU. The following functions are required for performing the message exchange operations between the host and the NIU:

a. Serial and parallel data transformation

b. Data path establishment

c. Store messages from the host and relay the messages to the communication channel

d. Store messages from the network channel and relay them to the host

The serial and parallel data transformation function is required because the host is connected to the NIU through its serial port. Data may flow in or out to the node. Data may also flow inside the node. The establishment of the data path determines the data routes. If the host wants to transmit messages to other nodes and its NIU currently does not hold the token, then the messages must be stored in the NIU transmitter buffer to be relayed later to the network. When messages come from other nodes addressed to the host, the host may be busy. The NIU receiver buffer is used for storing these messages. These messages are relayed to the host when it is idle.

4.3.3 Device Oriented Functions

Remember that COLAN is a control oriented LAN, therefore, device control functions are also important system components. In COLAN, serial and parallel communication ports are provided for connecting devices to the NIUs. A task library is also provided for performing some general purpose control operations. Because of the highly device-dependent property of control applications they will not be discussed.

4.3.4 NIU Implementation

According to the requirements discussed above and the low cost consideration, a single chip control oriented microcomputer, the 8031 with support chips was selected for implementing the NIU. The functional block diagram of an NIU is shown in Fig.4-7.

The hardware implementation of an NIU has been carried out and its hardware block diagram is given in Fig.4-8. In this implementation, the bus interface port employs the 8031 microcomputer on chip serial communication port. This serial port has a "wake up" feature. The receiver might respond only upon receiving address data. For other unrelated data communication, the port will not interrupt the micro-computer. This feature allows the unrelated nodes to concentrate on their own operations rather than be interrupted frequently by unrelated data transmissions. An Intel 8251 serial communication port is provided for the NIU to communicate with its host. External program memory and data memory are provided for use as the network operating system program memory, command storage memory, and transmitter and receiver buffers. A programmable peripheral interface (PPI) chip (Intel 8255) and an IO Port chip (Intel 8155) have been provided for connecting other communicating devices.

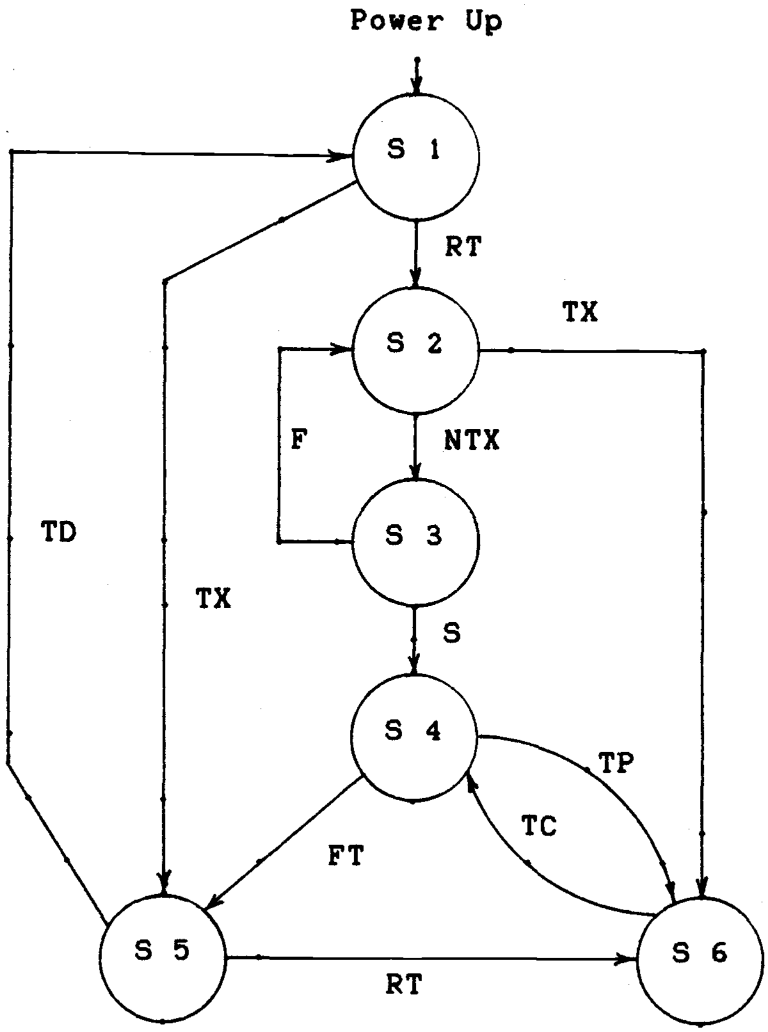


Fig.4-1. COLAN Control State Diagram

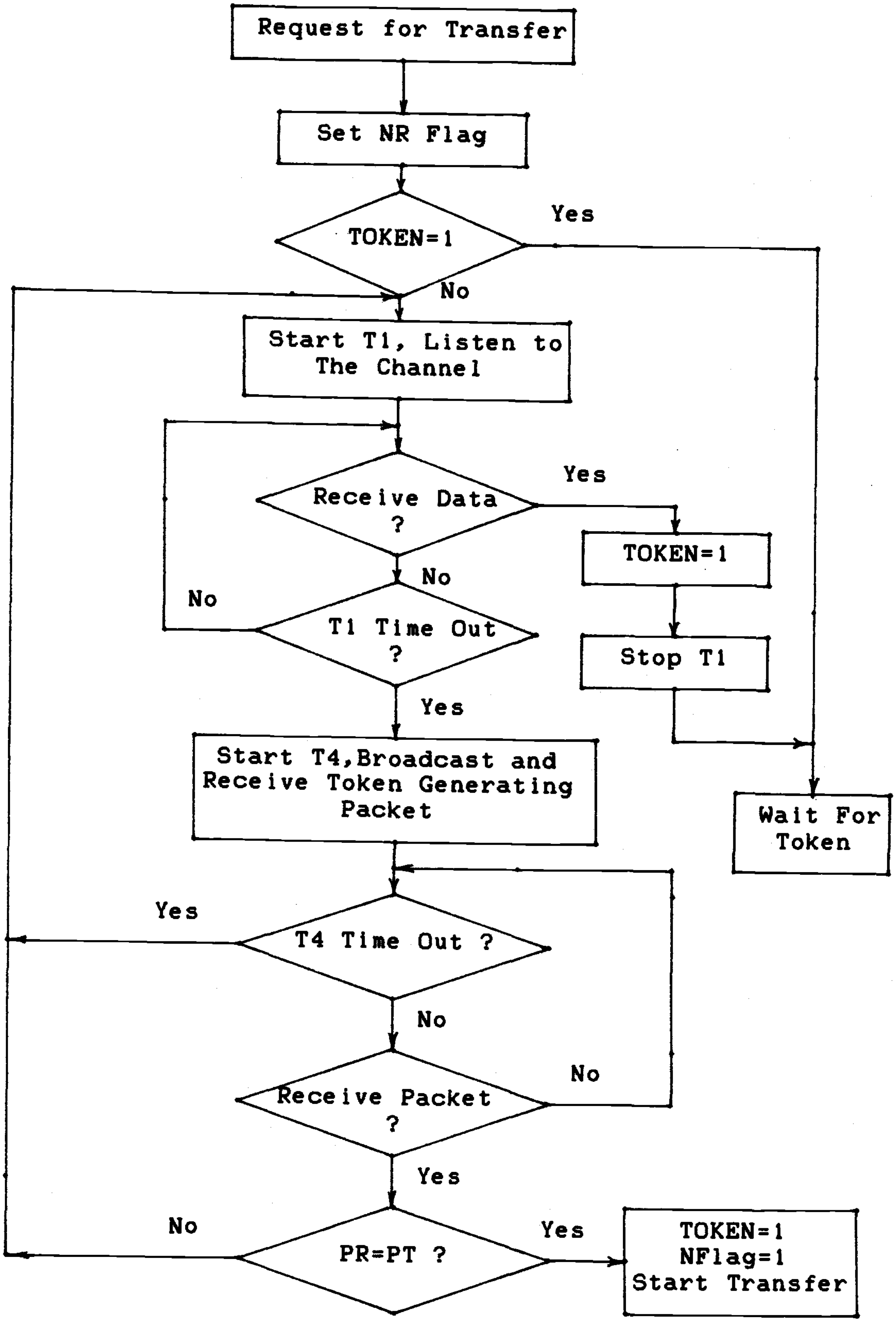


Fig.4-2. Token Generating Flow Chart

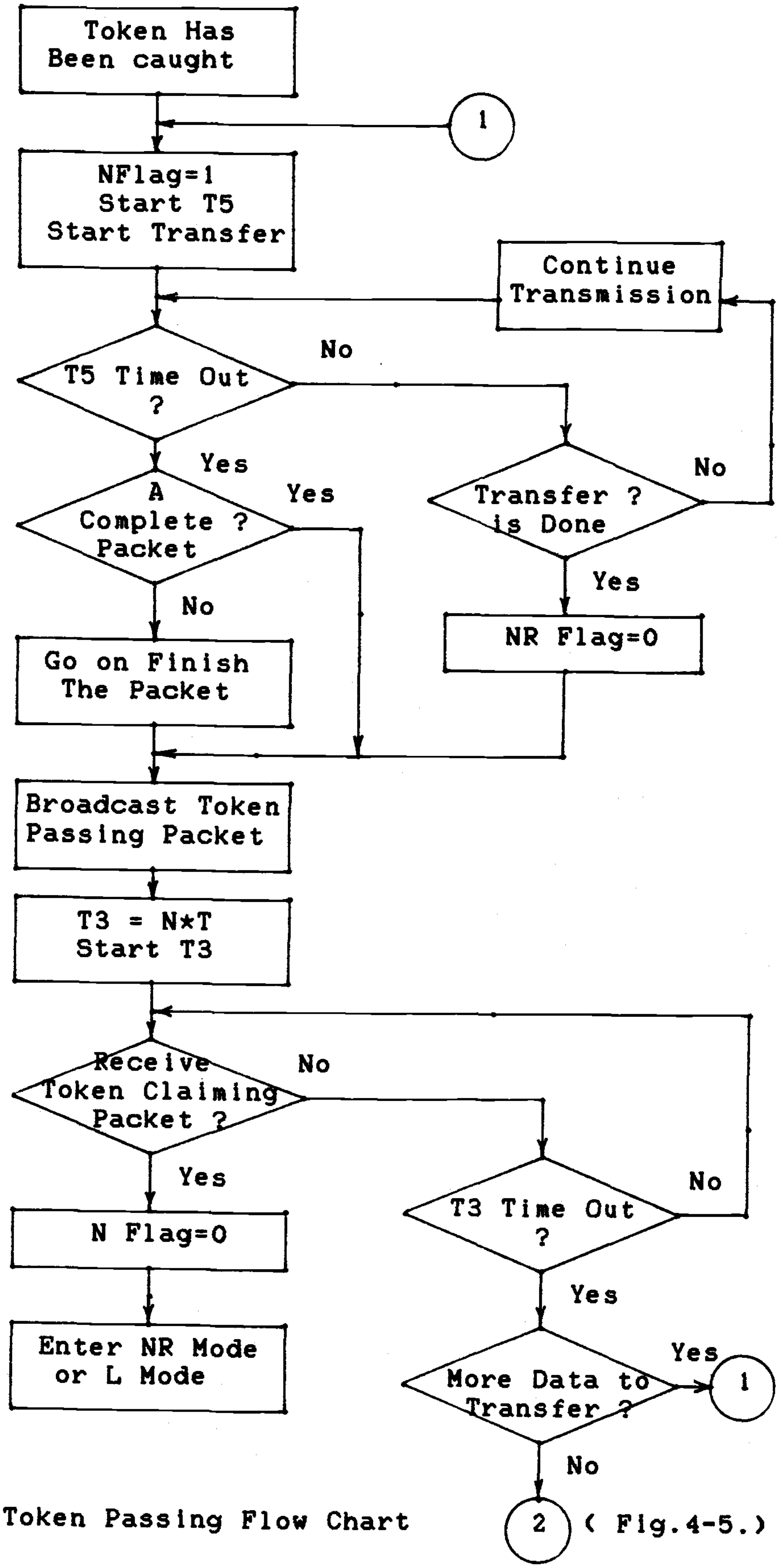


Fig.4-3. Token Passing Flow Chart

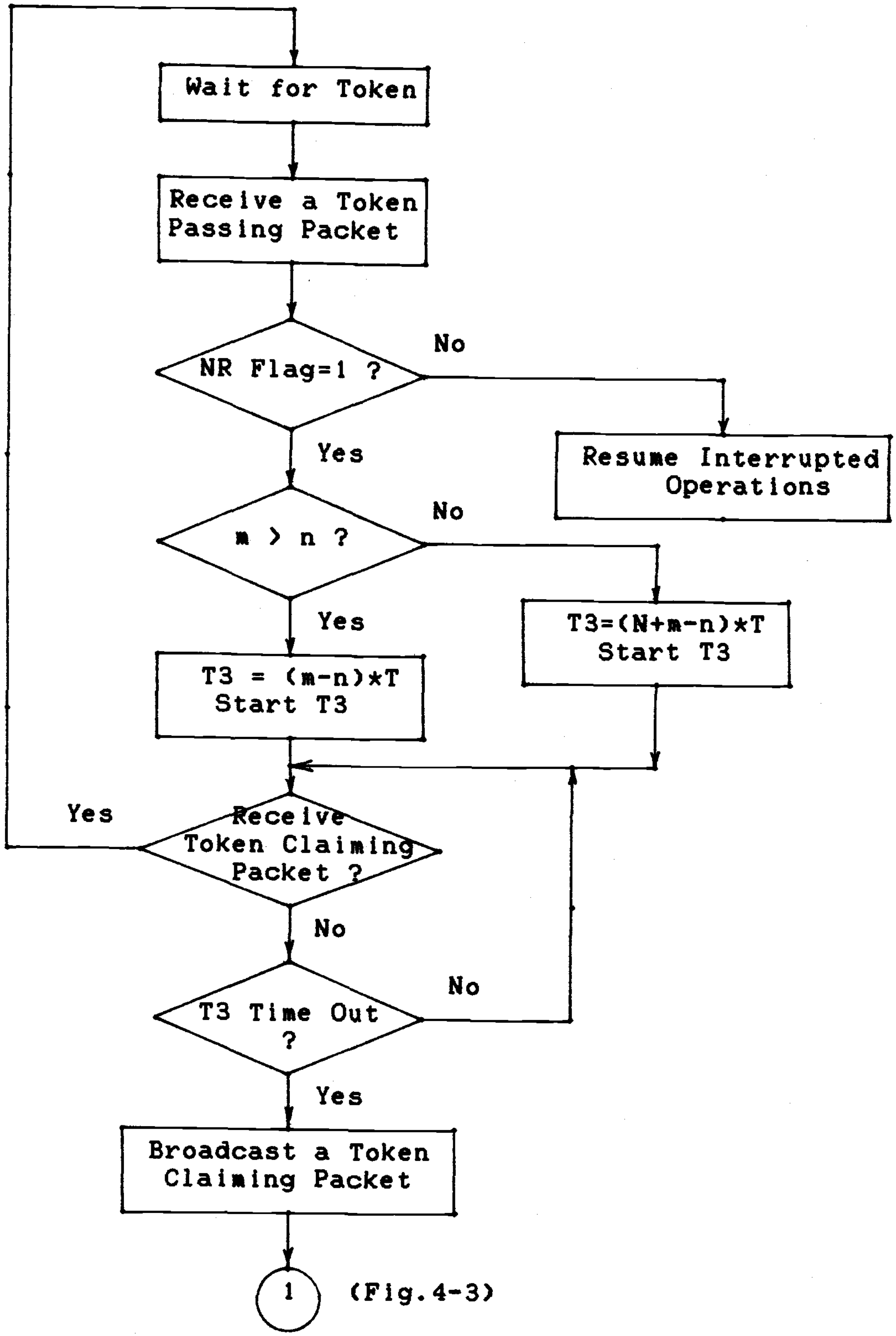


Fig.4-4. Waiting for Token Flow Chart

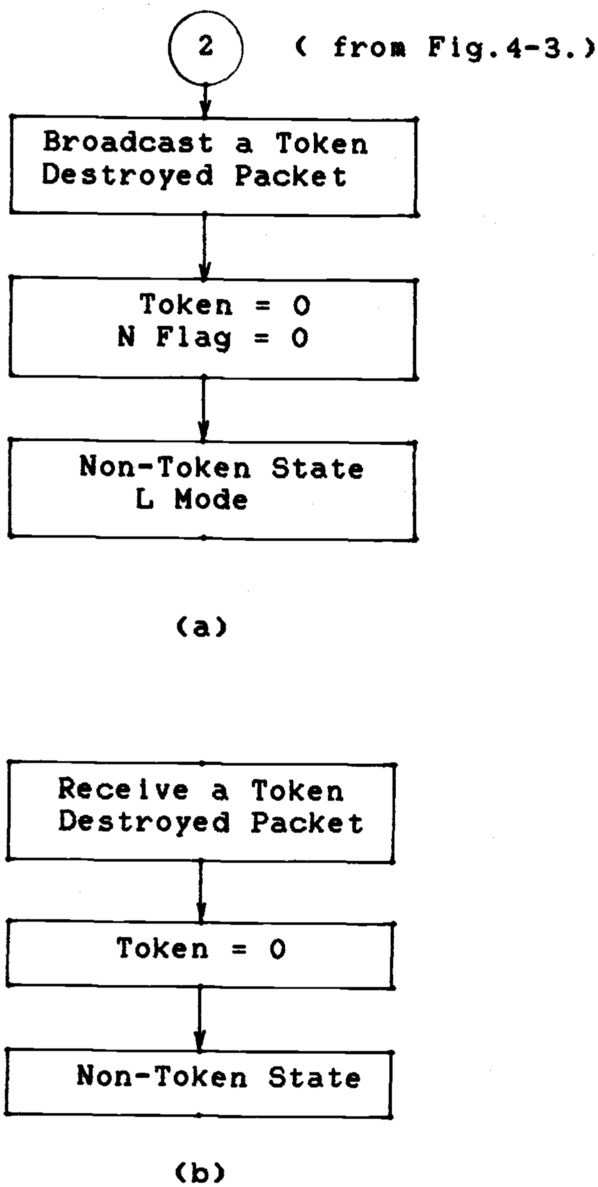


Fig.4-5. Destroying the Token
(a) for Token Holder
(b) for Non-Token Holder

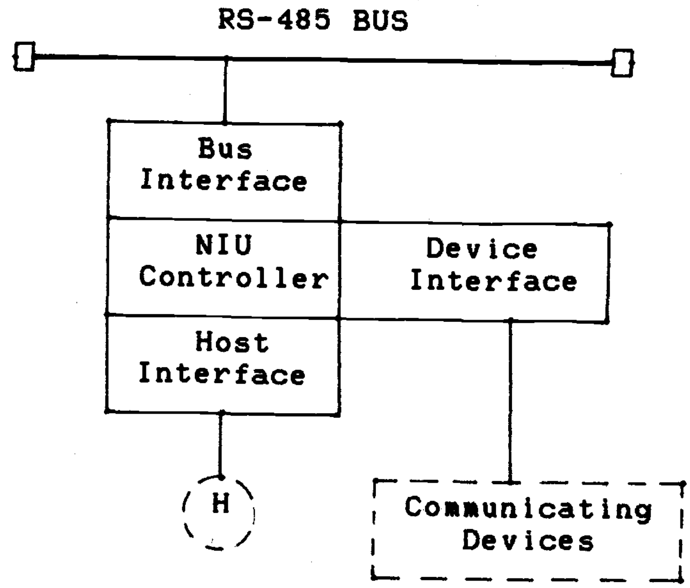


Fig. 4-6. Conceptual Configuration of An NIU

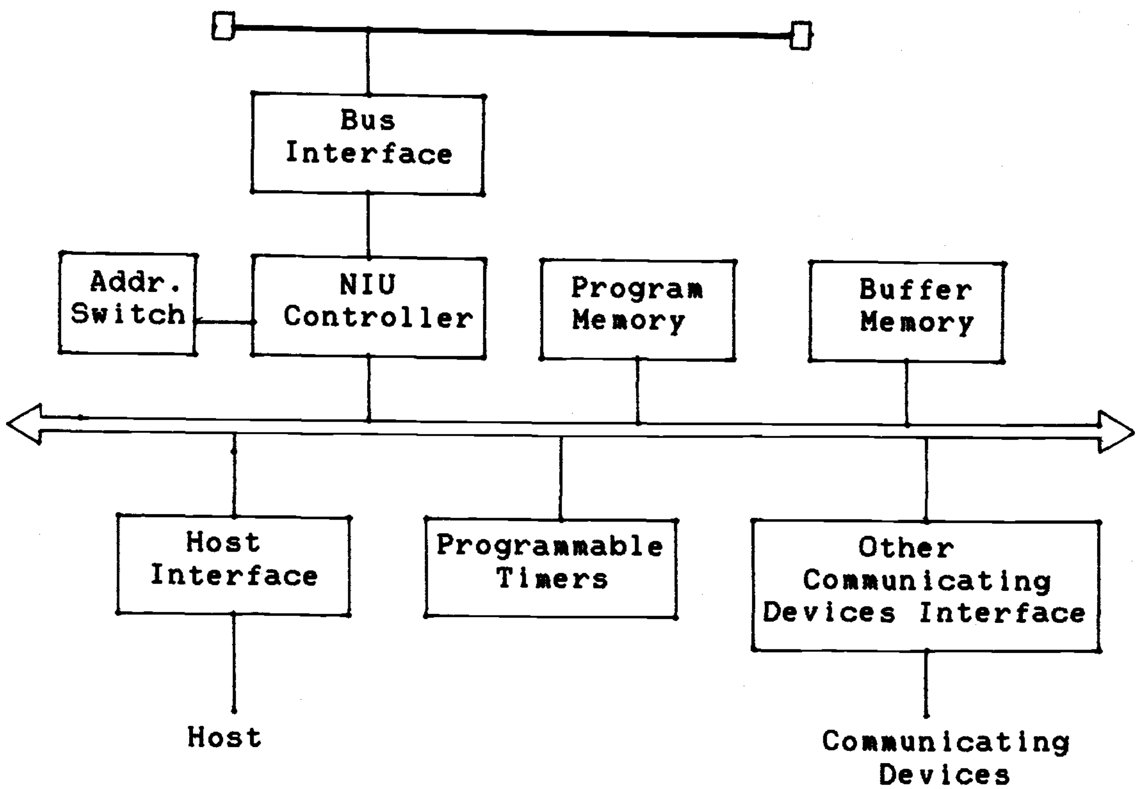
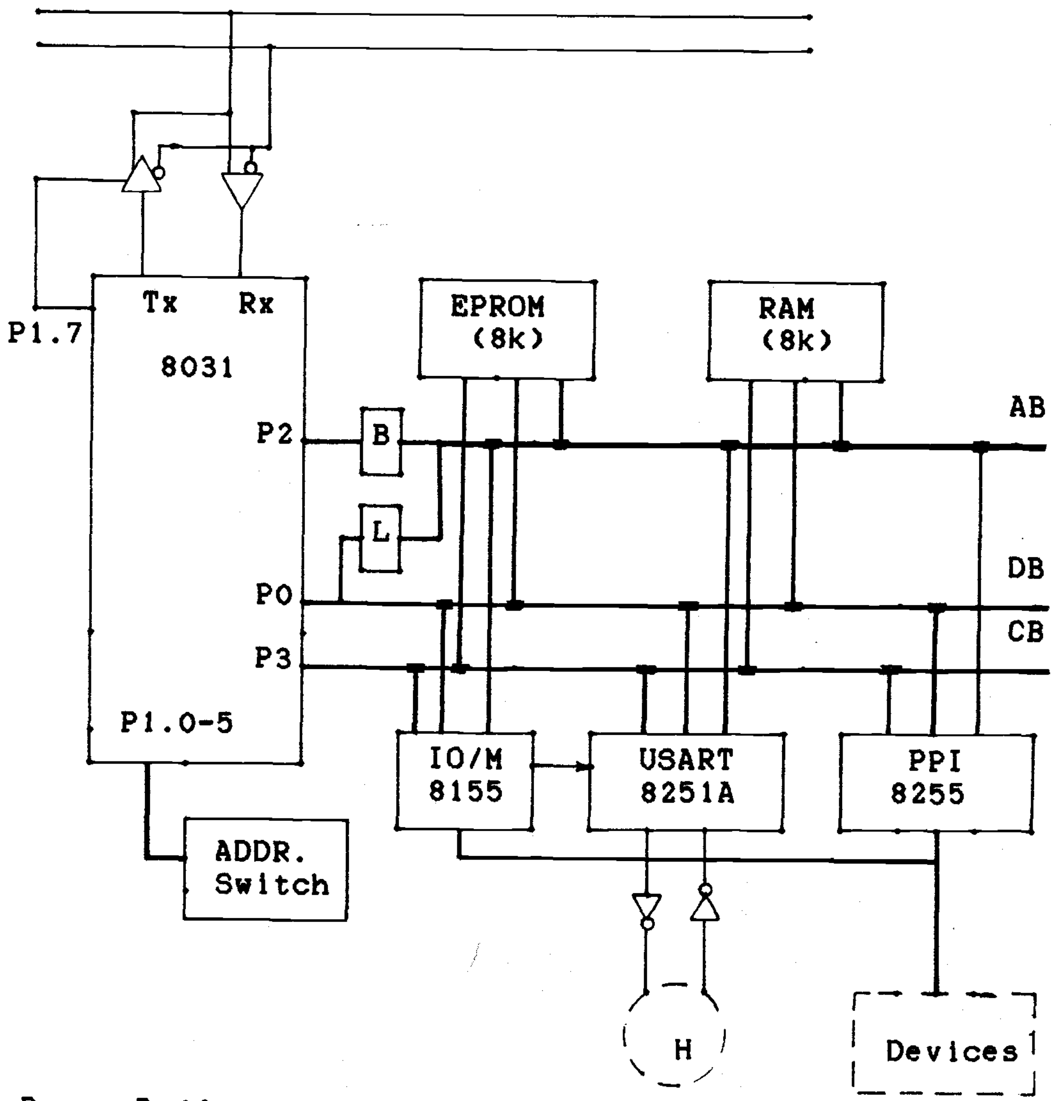


Fig. 4-7. Functional Block Diagram of An NIU



B --- Buffer
L --- Latch
AB --- Address Bus
DB --- Data Bus
CB --- Control Bus
H --- Host

Fig. 4-8. NIU Hardware Diagram

CHAPTER 5 SUMMARY AND FUTURE DEVELOPMENT

The previous chapters of this dissertation discussed the design of the COLAN --- the Control Oriented Local Area Network. The primary goal concerning the design of the COLAN was to improve the performance of the Task-Masters and let devices to talk to one another. The problems of most concern in the design of the COLAN were low cost and simplicty. Therefore, after the bus topology was selected, most research activities were devoted to the development of a simple communication channel access control protocol. Designing and implementing a Network Interface Unit were also important parts of the research activities.

As the result of this effort, a hybrid channel access control protocol, which combines the CSMA/CD technique and the token bus technique, has been developed. The hardware circuit of a Network Interface Unit (NIU) has also been implemented. Now, with this NIU and a modified Task-Master, two personal computers can communicate with each other.

Compared to the pure CSMA/CD and pure token bus techniques, this hybrid control protocol has the following advantages:

1. Shorter delay time compared to token bus when traffic is light.
2. Don't need a specific node to monitor the operation of the network, such as generating the control token, recovery from lost token. These functions are equally distributed among all of the nodes.

This distributed control mechanism makes the network capable of operating properly under any combination of the nodes, and therefore makes the network more robust than a token bus.

3. When the load of the network is heavy, it operates as a token bus and therefore has higher throughput and more stable than CSMA/CD contention bus.

Compared to the Task-Masters, the performance of the COLAN has been improved greatly in respect to the three items mentioned in chapter 1. COLAN also provides more device interfaces for control applications.

Ideally, when the load of the network is light, COLAN would operate like a CSMA/CD bus network. With the network traffic growing heavier, the delay-throughput characteristic of the CSMA/CD bus will meet the token bus delay-throughput characteristic. When the traffic is heavier than this load, COLAN would operate like a token bus. This would be the optimized delay-throughput characteristic of this hybrid control protocol. Unfortunately, because of the matter of time, no effort has been exercised to optimize this characteristic. The technique used in COLAN to decide when to use CSMA/CD and when to employ token bus has not been simulated by any method. It is likely that control scheme employed in COLAN might not be the optimized one. It is worthwhile to study this delay-throughput characteristic and simulate it by computer program. It would be very significant if the best time for the network to switch from one protocol to the other is found.

Without the following further research activities, the implementation of the COLAN would not be finished:

1. Implement more Network Interface Units. Only one has been implemented so far.
2. Develop the network operating system. With two or more NIUs, it is possible to develop the the network operating system and test it out.
3. Develop the library of tasks for control applications. Without this library, COLAN can not be used for control applications.

CHAPTER 6 BIBLIOGRAPHY

ABBA 85 Abbadi, A.E., and Rauchle, T., " A Resilient Communication Structure for Local Area Networks," Proc. Computer communication Review, Vol.15, No.4, Sept.1985, pp.140-145.

ABRA 70 Abramson, N., "The ALOHA System -- Another Alternative for Computer Communication," Proc. FJCC, 1970, pp.281-285.

ABRA 77 Abramson, N., "The Throughput of Packet Broadcasting Channel," IEEE Trans. Commun., Vol. VOM-25, Jan. 1977, pp.117-128.

ANDR 82 Andrews, D.W.,and Sshultz, G.D., "A Token-Ring Architecture for Local-Area Networks: An Update," Proc. of COMCON F'82, 1982, pp.615-624.

BART 85 Bartee, T.C., "Data Communications, Networks, and Systems," Howard W. Sam & Co., Inc. 1985.

BLAS 86 Blass, D., and Thanawastien, S., "A CSMA/CD-Token Ring Local Network Architecture with CSMA/CD-DAMA Protocol" INFOCOM'86, IEEE Computer Society 1986, pp.76-84.

BOUL 85 Boulton, P.I.P., and Lee, E.S., "Bus, Ring, Star and Tree Local Area Network," Computer Communication Review, May 1985, pp.19-24

BUX 81 Bux, W., "Local Area Subnetworks: A Performance Comparison," IEEE Transactions on Communication, Vol. COM-29, No.10, Oct.1981, pp.1465-1473.

CARL 86 Carlos, B.D., and Winkler, J., "Token Ring Local Area Network Management," INFOCOM'86, IEEE Computer Society, 1986, pp.94-98.

CHIO 86 Chiou,I.Y.,and Liu, M.T., "Gateway: A Voice/Data Internet Transport System," INFOCOM'86,IEEE Computer Society, 1986, pp.39-46.

CHOR 84 Chorafas, D.N., "Designing and Implementing Local Area Networks," McGraw-Hill, Inc. 1984.

COTT 80 Cotton, I.W., "Technologies for Local Area Computer Networks" Computer Networks, Nov.1980, pp.197-208.

CROW 86 Crowder, R.S., "Map, Proway, and IEEE 802: A Marriage of Standards for automation," INFOCOM'86, IEEE Computer Society 1986, pp.337-342.

ELLI 83 Ellis, G., Dillon, S., Stritter, S., and Whitnell, J., "Experience with Layered Approach to Local Area Network Design," IEEE Journal on Selected Areas in Communications, Nov. 1983, pp.857-868.

FARM 69 Farmer, W.D., Newhall, E.E., "An Experimental Distributed Switching Systems to Handle Bursty Computer Traffic," Proc. ACM Symp on Problems in the Optimization of Data Communications Systems, Oct. 1969, pp.1-33.

FARO 86 Farowich, S.T., "Communication in the Technical Office" Spectrum, April 1986, IEEE Inc..

FLIN 83 Flint, D.C., "The Data Main Ring: An Introduction to Local Area Networks," Wiley Heyden Ltd. 1983, London.

GEE 82 Gee, K.C.G., "Local Area Networks," The National Computing Center Limited, 1982, England.

GEOR 86 Georganas, N.D., and Naffah, N., "Integrated Office Systems over Local Area Networks: A Performance Study," INFOCOM'86, IEEE Computer Society 1986, pp.155-161.

GORD 80 Gordon, R.L., Farr, W.W., and Levine, P., "Ringnet: A Packet Switched Local Area Network with Decentralized Control," Computer Networks, Vol.3, 1980, pp.373-379.

GOUD 86 Gouda, M.G., and Sastry, A.R.K., "Broadcasting Finite State Machines: for Modeling LAN Protocal," INFOCOM'86, IEEE Computer Society 1986, pp.58-66.

GUPT 86 A. Gupta, "New Developments and Applications of Microcomputer Hardware and Software," Handbook of Information Technology and Office Systems, Elsevier Science Publishers B.V. 1986, New York, pp.651-676.

HAFN 74 Hafner, E.R., Nenada, Z., and Tschanz, M., "A Digital Loop Communication Systems," IEEE Trans. on Communications, Vol. COM-22, June 1974, pp.877-881.

JANS 83 Janson, P., Svobodova, L., and Maehle, E., "Filing and Printing on a Local Area Network," Proc. Computer Communiation Review, Vol.13, No.4, 1983, pp.211-219.

JUAN 86 Juang, J.Y., and Wah, B.W., "Channel Allocation in Multiple Contention Networks," INFOCOM'86, IEEE Computer Society, 1986, pp.189-196.

KAMA 86 Kamal, A.E., and Hamacher, V.C., "Analysis of A Star Local Area Network with Collision Avoidance," INFOCOM 86, IEEE Computer Society 1986, pp.546-555.

KAMI 86 Kaminski Jr., and M.A., "Protocols For Communicating In The Factory," Spectrum, April 1986, IEEE Inc.

KANG 81 Kang, Y.J., "A Distributed Local Computer Network: FISHNET- Facilities Integrated in a Shared Habitat NETwork," Ph.D Dissertation, Oregon State University, Corvallis, Oregon, 1981

KANG 86 Kang, Y.J., Springs, J.D., Jafari, H., and Herzog, J.H., "A New Approach To Mesh Local Area Network Routing," INFOCOM'86, IEEE Computer Society 1986, pp.106-114.

KELL 84 Kelley, R., Jones, J.,Bhatt, V., and Pate, P., "Transceiver Design and Implementation Experience In An Ethernet Compatible Fiber Optic Local Area Network," Proc. of INFOCOM'84, 1984, pp.2-7.

KLEI 82 Kleinrock, L., "A Decade of Network Development," Journal of Telecommunication Networks, Spring 1982, pp.1-11, Computer Science Press Inc..

KUMM 82 Kummerle, K., and Reiser, M., "Local Area Communication Networks - An Overview," Journal of

Telecommunication Networks, Winter 1982, pp.349-370.

LAM 80 Lam, S.S., "A Carrier Sense Multiple Access Protocol for Local Networks," Computer Networks, Vol. 4, 1980, pp.21-32.

LAM 84 Lam, S.S., "Fundamentals of Computer Communication Networks," Tutorial: Principles of Communication and Networking Protocals, pp.1-42, IEEE Computer Society Press, 1984.

LICK 78 Licklider, J.C.R., and Vezza, A., "Application of Information Networks," Proc. of the IEEE, November 1978, pp.1330-1346.

LIND 82 Lindsay, D.C., "Local Area Networks: Bus and Ring vs. Coincident Star," Computer Communication Review, Vol. 12, #3 & 4, July - Oct. 1982, pp.83-91.

LIU 78 Liu, M.T., "Distributed Loop Computer Networks," Advances in Computers, Vol.17, (M.C. Yovits, editor), pp.163-221, Academic Press, New Youk, 1978.

LIU 81 Liu, M.T., Tsay, D.P., Chou, C.P., and Li, C.M., "Design of The Distributed Double-Loop Computer Network (DDLCN)," J. Digital Systems, Vol.5 (Spring/summer 1981), pp.3-37.

LIU 84 LIU, M.T., and Rouse, D.M., " A Study of Ring Networks," Elsevier Science Publishers B.V. 1984.

LUCZ 78 Luczak, E.C., "Global Bus Computer Communication

Techniques," Proc. Computer Networking Symp. pp.58-67, Nat. Bar. Std, 1978.

MALH 86 Malhotra, M.K., and Omidyar, C.G., "Trends and Issues In Local Area Networks," INFOCOM'86 IEEE Computer Society 1986, pp.123-129.

MEDI 86 Meditch, J.S., and Yin, D.H.-L., "Performance Analysis of Virtual Time CSMA," INFOCOM'86 IEEE Computer Society 1986, pp.242-251.

MEIJ 82 Meijer, A., and Peeters, P., "Computer Network Architectures," Computer Science Press, Inc. 1982

MEIS 77 Meisner, N.B., "Dual-mode Slotted TDMA Digital Bus," Proc. Data Comm. Symp. 5th, Sept. 1977, pp.5-14 -- 5-18.

METC 83 Metcalfe, B. "Controller/Transceiver Board Drives Ethernet Into PC Domain," Mini-Micro Systems, January 1983, pp.179-190.

NEED 82 Needham, R.M., and Herbert, A.J., "The Cambridge Distributerd Computing Systems," Addison-Wesley Publishing Co., Reading Mass., 1982

PAUL 80 Paulish, D.J., "A Fail-Soft Distributed Processing System," Proc.COMPCON Fall'80, Sept.1980, pp.179-184.

PIER 72 Pierce, J.R., "Network or Block Switching Of Data," BSTJ, Vol.51, July-Aug. 1972, pp.1133-1145

PIRK 86 Pirkul, H., "Location of Concentrators In Designing Local Access Networks," INFOCOM'86 IEEE Computer Society 1986, pp.148-154.

PITT 86 Pitt, D.A., "Current and Future Medium Access Control Standards," INFOCOM'86 IEEE Computer Society 1986, pp.319-322.

PITT 86 Pitt, D.A., and Farazaneh, F., "Topologies and Routing For Bridged Local Area Networks," INFOCOM '86 IEEE Computer Society 1986, pp.34-38.

ROHL 83 Rohling, T., "ARCNET: Design and Implementation of A Local Network," Proc. of INFOCOM'83,1983, pp.512-517.

SALT 81 Saltzer, J.H. Clark, D.D., and Pogran, K.T., "Why a Ring ?" Proc. of the Seventh Data Communications Symp. 1981, pp.211-217.

SCHE 83 Scherr, A.L., "A Perspective on Communications and Computing," IBM Systems Journal, Vol.22, Num.1/2, 1983, pp.5-9.

SHEN 86 Shen, S.H., and Liu, H.T., "Dynamic CSMA/CD with A Priority Scheme," INFOCOM'86 IEEE Computer Society 1986, pp.258-263.

SHOC 82 Shoch, J.F., Dalal, Y.K., Redell, D.D., and Crane, R.C., "Evolution of The Ethernet Local Computer Network," Computer, Aug. 1982, pp.10-26.

SING 84 Singh, I.M., "Implementation of Standard LAN Protocols-Tools For Development and Verification," Proc. of COMPCOM s'84, 1984, pp.261-265.

STAL 84 Stalling, W., "Local Networks An Introduction," Macmillan Publishing Company, 1984, N.Y.

STUC 83 Stuck, B.W., "Calculating The Maximum Mean Data

Rate In Local Area Networks," Computer, Vol.6, Num.5, May 1983, pp.72-76, IEEE Inc.

SUNS 79 Sunshine, C., "Formal Techniques For Protocol Specification and Verification," Computer, Sept. 1979, pp.20-26.

TANE 81 Tanenbaum, A.S., "Computer Networks," Prentice-Hall, Inc. 1981.

TANG 86 Tang, Y.J., and Zaky, S.G., "A Unified Queueing Model For Performance Evaluation Of Local Ring Networks," INFOCOM'86 IEEE Computer Society 1986, pp.556-563.

TROP 81 Tropper, C., "Local Computer Network Technologies" Academic Press, Inc. 1981, N.Y.

TUCK 82 Tucker, J., "The Lower Layers of The OSI Reference Model," Proc. of the Sixth International Conference on Computer Communication, Sept.1982, pp.849-853.

VRAN 81 Vranesic, Z.G., Hamacher, V.C., Loucks, W.H., and Zaky, S.G., "TORNET: A Local Area Network," Proc. ACM 7th DATA COMM., Nov. 1981, pp.318-322.

VOEL 86 Voelcker, J., "Helping Computer Communication," Spectrum, March 1986, IEEE Inc.

WANG 83 Wang, P.S-C., and Kimbleton, S.R., "A Function Oriented Corporate Network," Proc. : Computer Communication Review, Vol.13, No.4, Oct. 1983, pp.203-210.

WHIT 86 White, J., "Advances In Semiconductor Technology," Handbook of Information Technology and Office Systems, Elsevier Science Publishers B.V., 1986

YOUN 86 Young, I., "Progress In Office Systems," Handbook of Information Technology and Office Systems, pp.803-814, Elsevier Science Publishers B.V. 1986

ZELE 84 Zeletin, R.P., "Some Critical Considerations On The ISO/OSI RM From A Network Implementation Point Of View," Proc. Computer Communication Review, Vol.14, No.2, June 1984, pp.188-194