Reliable Ethernet Architecture with Redundancy Scheme for Railway Signaling Systems

Jong-Gyu Hwang* and Hyun-Jeong Jo†

Abstract – Recently, vital devices of the railway signaling systems have been computerized in order to ensure safe train operation. Due to this computerization, we have gradually come to need networking interfaces between these devices. Thus it is important that there be reliable communication links in the signaling systems. Network technologies are applied in the real-time industrial control system, and there are numerous studies to be carried out on the computer network technology for vital control systems such as railway signaling systems. For deploying the studies, we consider costs, reliability, safety assurance technique, compatibility, and etc. In this paper, we propose the Ethernet for railway signaling systems and also precisely describe the computer network characteristics of vital railway signaling systems. Then we demonstrate the experimental results of the proposed network algorithm, which is based on switched Ethernet technology with redundancy scheme.

Keywords: Railway signaling systems, Redundancy scheme, Switched Ethernet

1. Introduction

Railway signaling systems are computerized vital systems for the safety guarantee of train operation, which controls train speed and direction, especially preventing train collisions, located about the side of rails. Every signaling system plays each role, and is linked with other signaling systems; finally constructing a bigger signaling system.

The links between controlling devices for railway signaling have some problems in regards to maintenance and repairs and the addition of new equipment because the linking method is point-to-point communication. Recently, railway advanced countries are trying to study and develop a way of linking signaling systems by networking them, and some countries have already begun to use this networking method [1, 2].

The advent background of studying the railway signaling system network, with a view of science technology, is that there are increasing needs for transmitting data between railway signaling systems. The increasing needs of the networking technology that satisfies real-time requirements and has reliability in the high quality systems, like railway signaling systems, can be another background.

Ethernet application to industrial controlling systems was impossible because the real-time requirements were not satisfied owing to the random characteristics of the Ethernet protocol, but the recently advanced switched Ethernet enables the Ethernet technology to be applied to industrial controlling systems [3]. By the theoretical explanations of the switched Ethernet, we identify the possibility of applying it to railway signaling systems.

Also, the vital controlling systems, such as railway signaling systems, require higher reliability than the general industrial controlling systems. In this paper, we analyze the performing efficiency through an Ethernet-based network algorithm, which has high reliability, including the algorithm for detecting faults and its recovery when network defects occur.

If the proposed Ethernet-based network algorithm is applied to interfaces between railway signaling systems, much development of the extension, and the maintenance and repairs of the signaling control systems can be expected, and so do consistent operation of signaling control systems accompanied by guaranteeing the communication system reliability.

2. Review of Industrial Network Technology

Industrial network technologies have been earnestly developed from the mid 1980's, and current IEC 61158 international standards, including several protocols, such as Profibus, Fieldbus Foundation, WorldFIP, and others, have been established. Furthermore, network technologies for Ethernet-based industrial control systems, such as RETHER, 3Com PACE, HP AnyVG LAN, and IEEE 802.1p, which are MAC class mechanisms for supporting

† Corresponding Author: Train Control System Research Team, Korea Railroad Research Institute, Uiwang-city, Gyounggi-do, Korea (hjjo@krri.re.kr)

* Train Control System Research Team, Korea Railroad Research Institute, Uiwang-city, Gyounggi-do, Korea

Received 28 February,2006 ; Accepted 17 November, 2006

the real-time traffic, are studied. To apply industrial networks to railway signaling systems, choosing appropriate protocols should include considering various elements.

On a broad scale, cost, data transmission rate, extensibility, supporting media, the ways of media connection, and other elements should be considered. Considering these elements, the network of railway signaling systems is consequently determined to be developed by Ethernet-based protocol.

Railway signaling systems require higher reliability and safety than the industrial controlling systems. The direct applications of the network technologies, which are used for general control equipments, are dangerous. In other words, the network technologies, which have high reliability and safety for the uses of railway signaling systems, are necessary.

The efficiency of Ethernet-based protocols has already been acknowledged in many industrial fields, and various methods to develop the reliability have already been studied. The reason is that general industrial network-systems are developed by adapting the requirements and the automation environment of field applications, but the current trend comes from relating communication technologies with automation.

The Ethernet appears as the next generation industrial network because of its open structure and low cost. Recently, the switched Ethernet shows a very promising prospect for industrial networking because the switching technology can eliminate frame collisions. Because the Ethernet without collisions is no longer unstable under heavy traffic and its delay can be drastically reduced, the adoption of switched Ethernet as an industrial network is seriously considered along with the appearance of inexpensive switches [4].

3. Mathematical analysis of Ethernet for railway signalling systems

If these Ethernets are directly applied to the railway signaling systems, and transmitted data do not have regular transmission delays, then the Ethernets problematically have random transmission delays, namely uncertainty of transmission delays. And, the methods to reduce the number of collisions in the Ethernet also have problems, because people should modify data link classes or TCP/IP classes directly. In this paper, one problem of the Ethernet applications is solved by bringing the switching technologies as one way to solve the uncertainty of transmission delay in the Ethernet. The switching technologies were mainly developed and applied to the office network, but their trials for applying to industrial networks are increasing, as their generalization and cost decrease.

3.1 Ethernet and switched Ethernet

IEEE 802.3, often referred to as Ethernet, is developed for data communications among computers in the early 1970's by the IEEE, and is the basis of a physical layer and a data link layer of the office communication. Fig. 1 presents the communication procedure of the CSMA/CD (Carrier Sensing & Multiple Access/Collision Detection), which is the media access control method of IEEE 802.3.

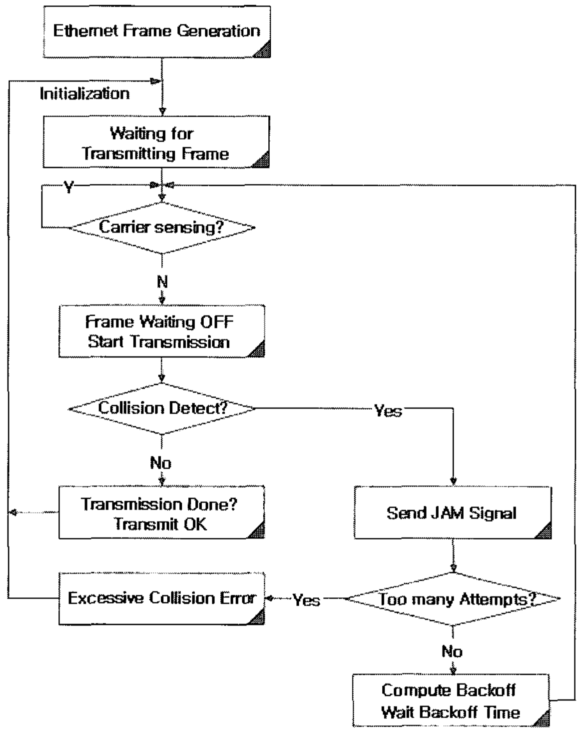


Fig. 1. The overview of CSMA/CD protocol

The source stations, which contain transmitting data, exam whether the media are used or not. If the media are used, the source stations delay transmitting, and wait until the media uses are finished (CS). If the media are not in use, the source stations transmit data frames (MA). In the case that any collisions are detected during the transmissions, the source stations stop the transmission, and send a jam signal of collision detection, and inform other stations of the collision occurrences (CD).

And it tries retransmission after the delay during the backoff time calculated by the BEB (truncated Binary Exponential Backoff) algorithm. These retransmission trails are occurred 16 times, and when the trial numbers are over 16 times, appropriate frames are abandoned. In the Ethernet, the more there are traffics by the CSMA/CD algorithm, the more collisions occur, so the transmission delays increase by waiting for the backoff time as long as the number of collisions. And also, the delaying time cannot be predicted because of the delaying by the random time following the BEB algorithm [3, 5].

The switched Ethernet differs from the conventional one. In the switched Ethernet, collisions between other stations are prevented because the dedicated virtual circuits between the stations, which communicate through switches, are installed. As we can see from Fig. 2, collisions do not occur in the cases of which many stations transmit simultaneously because the switches send frames only to the determined destination stations when the source stations transmit frames. As well, other collisions are not occurred before the frames are received because the full duplex method is used in the switched Ethernet, which performs sending and receiving by each line.

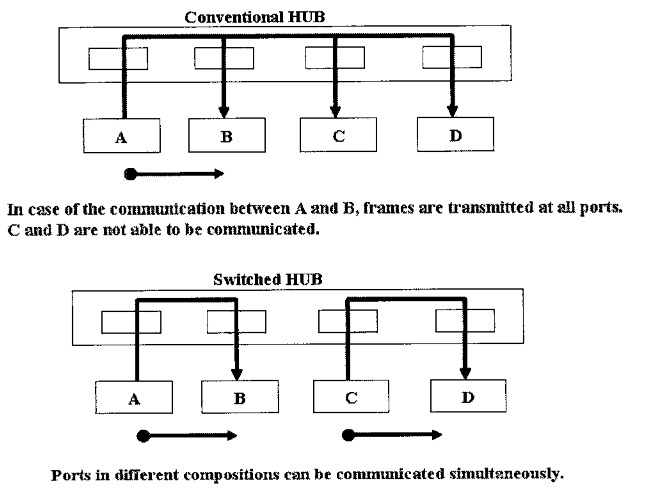


Fig. 2. Comparison of conventional Ethernet and switched Ethernet

A typical method of switching technology is the store and forward method. In Fig. 2, the switch receives a frame through the transmission line from a source station, and then checks if the reception line of a destination station is idle. If the reception line is idle, the switch transmits the frame. Otherwise, the switch stores the frame into its buffer and waits until the reception line becomes idle. In addition, if several frames with the same destination address are received at the switch simultaneously, the switch stores frames to the buffer and then sends frames to the destination one by one [6].

3.2 Theoretical analysis of maximum transmission delay for Ethernet and switched Ethernet

The performance analysis of the Ethernet has not yet been achieved exactly because of the probability characteristics of the BEB algorithm. In this paper, we theoretically analyze the maximum transmission delay of CSMA/CD, as one of the analysis methods by using the timing analysis of data link classes [7].

The maximum transmission delay of the existing Ethernet occurs in the following three kinds of situations; the maximum transmission delays occurs 1) after the transmitted frames collide 16 times, 2) when the backoff time has the greatest value, 2min (trial number 10), 3) when D_{DET} has the greatest value - twice the value of transmission delay between the source stations and the destinations. In these situations, the theoretical maximum collision delays are calculated as Equation (1).

$$\begin{aligned} D_C &= \sum_{k=1}^{16}(D_{DET}+D_{JAM}+D_{BO\max}) \\ &= 16(4D_{PROP}+D_{JAM})+\sum_{k=1}^{16}2^{\min(k,10)}t_s \\ &= (16(20+32)+(\sum_{k=1}^{9}(2^k-1)+\sum_{k=10}^{16}(2^{10}-1))\times 512)t_b \\ &= 4{,}185{,}920t_b \approx 418.6m\sec \end{aligned} \tag{1}$$

where t_b : Bit time (1/transmission speed)

$D_{BO\max}$: Maximum backoff time with BEB algorithm

D_{JAM} : Jam transmission time

D_{PROP} : Propagation delay

D_{DET} : Collision detection time

From the above analysis, we can identify that the maximum transmission delay occurring in the Ethernet is about $418.6m$sec. This result shows that the direct application to the industrial network is not proper because if the traffics of the Ethernet increase, the number of collisions and the following transmission delays drastically increase.

Theoretical maximum transmission delays of switched Ethernet occur when N_q value is maximum, which is determined by the network traffics and the quantity of switched buffer. If the network traffics are stable, and only the regular frames are generated, the value of N_q will be maximized because processing ability of switches per hour is big enough when the frames with the same destinations are generated simultaneously and stored in switches. The maximum transmission delay time D_Q is similar to that shown in Equation (2).

$$\begin{aligned} D_Q &= \sum_{k=1}^{N_q}(D_{IF}+D_{TK}) = \sum_{k=1}^{N_q}(D_{IF}+\max(L_k+L_h,576))t_b \\ &= N_q(96+\max(K_k+432,576))t_b \\ &= 13\times 672\times t_b = 873.6\mu\sec \end{aligned} \tag{2}$$

where D_{IF} : Interframe delay

D_{TK} : Message length of k^{th}

N_q : The number of frames stored in switches

L_k : Data size of k^{th}

L_h : Overhead of transmitted frames (10Base-T: 432 bit)

According to Equation (2), we can know that if the switched Ethernet is used, only a small transmission delay occurs. The reason of the result is that there is no collision in the switched Ethernet. The switched Ethernet satisfies the real-time requirements for the industrial networks, and it can be applied to railway signaling systems.

4. Network algorithm in railway signaling systems

In this paper, we study the methods of developing switched Ethernet reliability to apply them to railway signaling systems in which the safety is critical. Switched Ethernet satisfies the real-time requirements, but the reliability cannot be guaranteed when each component is broken down because system components are related with each other such as Network-Interface Card (NIC), switch HUB, and communication lines. To solve this problem, we propose the multiple architecture in which each component is duplicated, and then we estimate its performance.

4.1 Architecture of hardware redundancy

4.1.1 Switch HUB

In Ethernet communications, the data cables are shared, all nodes have their individual addresses, and the communications are also carried out by the addresses through switching HUBs. In the beginning stage of switching HUB, unavoidable collisions are occurred as traffics are gradually increasing because the HUB, which never buffers total packets, has just destination addresses and chooses the way to transmit. Most of the currently realized switching HUBs don't bring any collisions excluding queue delay in switches, because they have more than two independent queues in every port, and they store the entire data in the Store & Forward, transmitting it only after confirming destination addresses.

4.1.2 MultiPort Network Interface Card for fault-tolerant characteristic

Fault Tolerant is a system that is designed not to disturb system operations even in the case that some modules or components in the system have faults. The aim of the Fault Tolerant system is to continue operating the system regularly with no loss and destruction of data despite the occurrences of faults. The fault tolerance goes through the following three steps, each of which is preceded and linked with running application software.

1. Fault Detection

Fault Detection is usually operated by Compare Logic constructed by hardware. When faults appear in systems, the decided modules or the systems come into the fault-condition. When the faults appear, OS analyzes every condition of hardware modules, and identifies which module makes faults.

2. Fault Diagnosis

The characteristics of faults are transient or hard. If the faults are hard, the modules of the systems are removed. If they are transient, in which the self diagnoses result in no problem, the system first recognizes the fault as transient faults, and performs all operations.

3. Fault Recovery

Fault Recovery reconstructs systems by removing the modules which bring faults. One of the important functions, which maintains fault tolerance, is to duplicate data more than twice and then finally maintains the fault tolerance. In other words, when some data are created from application programs, the fault recovery always stores the data in two memories, and then transmits the data. Even when a module has some faulty data, fault recovery can maintain fault tolerance giving no influence on other systems. In this paper, we embody the Redundancy system by using NIC, which has four Modules.

4.1.3 System architecture with fault tolerance

As we mentioned above, to construct a fault tolerant system, multiple communication ports, and communication lines are needed. In addition, module redundancy should be embodied using multiple NIC, and redundancy in switches should be realized by linking switch HUBs doubly. If only one switch is installed, obstacles of total systems occur when faults are made in switches even though the redundancy in modules is guaranteed. Linking one communication line to one port each is another caution to

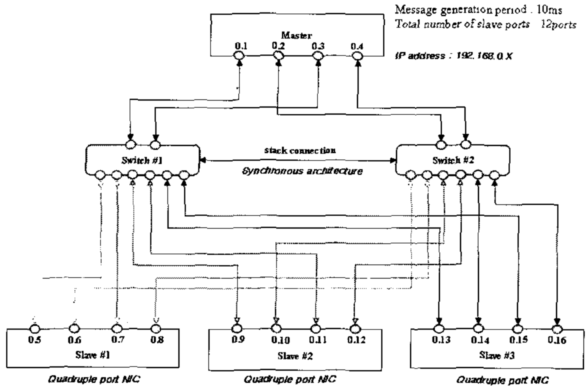


Fig. 3. Overview of System Architecture

avoid, because there is enough possibility to make errors in the communication lines. The following Fig. 3 is the system architecture that meets those requirements.

4.2 The development of fault detection and operation algorithm for communication nodes

In the switched Ethernet, to make components doubled, supporting software in application layer, such as the 7th level of OSI reference, is also necessarily needed in addition to the system framework of the hardware. At first, more than two bindings of network cards are supported in one station for the duplication of network cards, and more than two sockets and software buffers are required for communication.

The proposed system architecture uses four communication ports, four communication lines, and two switches, so the software for estimating the performance should be able to support system architecture. Fig. 4 is the approximate program diagram of the software for full redundancy of the switched Ethernet. Approximately explaining it, a slave which generates messages continuously creates messages per 10ms, and the message-generating routine creates an event of message generation to a slave message-sending routine when messages are generated. The slave message-sending routine that receives the event is constructed by the way of transmitting messages through individually binding ports. The master that receives the messages plays a role to carry perfect data to application levels after copying the data entered into individually received buffers. It then brings in voting routines and compares the data.

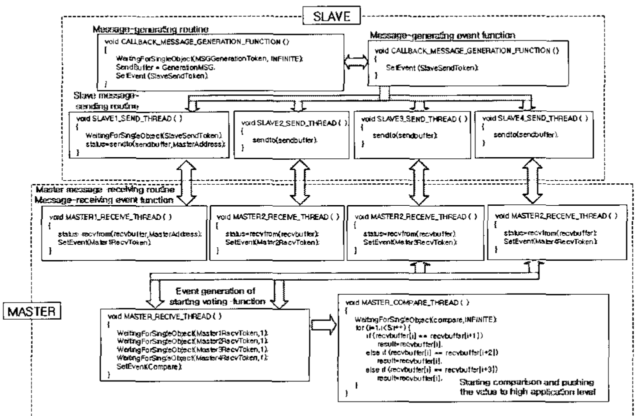
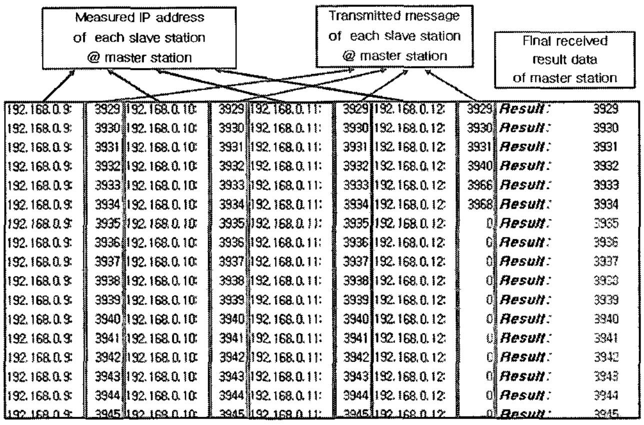


Fig. 4. Test software configuration of proposed Ethernet Architecture

5. Experimental analysis of proposed network algorithm

Bus redundancy is used to manage the conditions that some short circuits appear in cables by external causes from actual environments. Figs. 5 and 6 show the images of cables being cut, and the results achieved by the suggested system of this paper.

Fig. 5. Cutting cables



192.168.0.9:	3929	192.168.0.10:	3929	192.168.0.11:	3929	192.168.0.12:	3929	Result:	3929
192.168.0.9:	3930	192.168.0.10:	3930	192.168.0.11:	3930	192.168.0.12:	3930	Result:	3930
192.168.0.9:	3931	192.168.0.10:	3931	192.168.0.11:	3931	192.168.0.12:	3931	Result:	3931
192.168.0.9:	3932	192.168.0.10:	3932	192.168.0.11:	3932	192.168.0.12:	3940	Result:	3932
192.168.0.9:	3933	192.168.0.10:	3933	192.168.0.11:	3933	192.168.0.12:	3966	Result:	3933
192.168.0.9:	3934	192.168.0.10:	3934	192.168.0.11:	3934	192.168.0.12:	3968	Result:	3934
192.168.0.9:	3935	192.168.0.10:	3935	192.168.0.11:	3935	192.168.0.12:	0	Result:	3935
192.168.0.9:	3936	192.168.0.10:	3936	192.168.0.11:	3936	192.168.0.12:	0	Result:	3936
192.168.0.9:	3937	192.168.0.10:	3937	192.168.0.11:	3937	192.168.0.12:	0	Result:	3937
192.168.0.9:	3938	192.168.0.10:	3938	192.168.0.11:	3938	192.168.0.12:	0	Result:	3938
192.168.0.9:	3939	192.168.0.10:	3939	192.168.0.11:	3939	192.168.0.12:	0	Result:	3939
192.168.0.9:	3940	192.168.0.10:	3940	192.168.0.11:	3940	192.168.0.12:	0	Result:	3940
192.168.0.9:	3941	192.168.0.10:	3941	192.168.0.11:	3941	192.168.0.12:	0	Result:	3941
192.168.0.9:	3942	192.168.0.10:	3942	192.168.0.11:	3942	192.168.0.12:	0	Result:	3942
192.168.0.9:	3943	192.168.0.10:	3943	192.168.0.11:	3943	192.168.0.12:	0	Result:	3943
192.168.0.9:	3944	192.168.0.10:	3944	192.168.0.11:	3944	192.168.0.12:	0	Result:	3944
192.168.0.9:	3945	192.168.0.10:	3945	192.168.0.11:	3945	192.168.0.12:	0	Result:	3945

Fig. 6. Experimental results of bus redundancy

The experiment is to make 5,000 messages per 10ms, and the diagram shows the result achieved at a second (after about 39 seconds, in the experiment) when the cables of the slave whose IP address is 192.168.0.12 are cut. Up to the 3934th message, transmitting data per 10ms in stations increases by 1 gradually. Then there is no error and the final result value is normal.

However, when the cables are cut at the time of sending the 3935th message, the data are unable to be transmitted to masters. The 3935th data seems to be normally outputted because it is compared with other values in the masters. The entire number of normally generated messages is 20,000, the number of data with no error is 18,935, so the throughput of the data in this condition is 18,935/20,000 = 94.675%. The rate of message errors is seemingly 5.325%, and the rate of recovery is 100%. We can get the similar consequent rates of switch redundancy and of NIC module redundancy in the same conditions.

Transmission delay associated with the communication is a parameter that is the most importantly considered when we apply the network to the environments where the real-time proceeding is required. And it is a necessary element for indicating the performance standards of redundancy where objective standards have not yet been prepared. The time for detecting faults means the total time for sending messages from slave and analyzing them in masters. The fault detecting time covers transmission delay, which is the time for transmitting data from slave to master, and propagation delay, which also includes the processing delay used for analyzing data in masters. The measured time of transmission delay is similar to Equation (3).

2294	Address:	192.168.0.5	Data:	2293	Delay:	756.445	us
2295	Address:	192.168.0.5	Data:	2294	Delay:	759.56	us
2296	Address:	192.168.0.5	Data:	2295	Delay:	791.645	us
2297	Address:	192.168.0.5	Data:	2296	Delay:	793.284	us
2298	Address:	192.168.0.5	Data:	2297	Delay:	762.474	us
2299	Address:	192.168.0.5	Data:	2298	Delay:	759.282	us
2300	Address:	192.168.0.5	Data:	2299	Delay:	757.578	us
2301	Address:	192.168.0.5	Data:	2300	Delay:	759.205	us
2302	Address:	192.168.0.5	Data:	2301	Delay:	748.414	us
2303	Address:	192.168.0.5	Data:	2302	Delay:	772.204	us
2304	Address:	192.168.0.5	Data:	2303	Delay:	762.75	us
2305	Address:	192.168.0.5	Data:	2304	Delay:	758.755	us
2306	Address:	192.168.0.5	Data:	2305	Delay:	783.539	us
2307	Address:	192.168.0.5	Data:	2306	Delay:	791.097	us
2308	Address:	192.168.0.5	Data:	2307	Delay:	754.981	us
2309	Address:	192.168.0.5	Data:	2308	Delay:	773.953	us
2310	Address:	192.168.0.5	Data:	2309	Delay:	754.333	us
2311	Address:	192.168.0.5	Data:	2310	Delay:	755.035	us
2312	Address:	192.168.0.5	Data:	2311	Delay:	791.525	us
2313	Address:	192.168.0.5	Data:	2312	Delay:	755.354	us
2314	Address:	192.168.0.5	Data:	2313	Delay:	765.213	us
2315	Address:	192.168.0.5	Data:	2314	Delay:	759.315	us
2316	Address:	192.168.0.5	Data:	2315	Delay:	754.887	us
2317	Address:	192.168.0.5	Data:	2316	Delay:	751.896	us
2318	Address:	192.168.0.5	Data:	2317	Delay:	753.529	us
2319	Address:	192.168.0.5	Data:	2318	Delay:	759.869	us
2320	Address:	192.168.0.5	Data:	2319	Delay:	757.59	us
2321	Address:	192.168.0.5	Data:	2320	Delay:	761.359	us
2322	Address:	192.168.0.5	Data:	2321	Delay:	757.816	us
2323	Address:	192.168.0.5	Data:	2322	Delay:	774.907	us
2324	Address:	192.168.0.5	Data:	2323	Delay:	763.023	us
2325	Address:	192.168.0.5	Data:	2324	Delay:	771.603	us
2326	Address:	192.168.0.5	Data:	2325	Delay:	755.263	us
2327	Address:	192.168.0.5	Data:	2326	Delay:	752.094	us
2328	Address:	192.168.0.5	Data:	2327	Delay:	753.789	us
2329	Address:	192.168.0.5	Data:	2328	Delay:	765.081	us
2330	Address:	192.168.0.5	Data:	2329	Delay:	751.111	us
2331	Address:	192.168.0.5	Data:	2330	Delay:	752.815	us
2332	Address:	192.168.0.5	Data:	2331	Delay:	747.204	us
2333	Address:	192.168.0.5	Data:	2332	Delay:	762.799	us
2334	Address:	192.168.0.5	Data:	2333	Delay:	754.62	us
2335	Address:	192.168.0.5	Data:	2334	Delay:	763.461	us
2336	Address:	192.168.0.5	Data:	2335	Delay:	751.749	us
2337	Address:	192.168.0.5	Data:	2336	Delay:	755.933	us
2338	Address:	192.168.0.5	Data:	2337	Delay:	755.678	us

Fig. 7. Experiment of communication delay

$$\text{Fault detection time}(D_T) = \text{Transmission delay}(Comm_T) + \text{Propagation delay}(Prop_T) + \text{Processing delay}(Proc_T) \quad (3)$$

As we can see in the result from Fig. 7, the average transmission delay, which is measured from the traffic conditions where each 3 stations (each has four ports) generate data at 10ms, is about 770 μ sec. The fault detection time is within about 800 μ sec, because the faults are immediately identified without considering transient fault.

6. Conclusion

Railway signaling systems should necessarily guarantee reliability between the signaling systems because they are linked with other controlling equipments and construct bigger signal controlling systems, performing each function. The links of signaling systems have some problems in regards to maintenance and repairs because the linking method is point-to-point communication.

The safety-critical systems, such as railway signaling systems, signify the reliability with emphasizing transmission delay. For these necessities, fault tolerance should be realized in the environment, which requires high reliability when applying networks like cars, automobiles, and aviation vehicles. In this paper, we propose the reliable switched Ethernet architecture with redundancy systems and analyze the performing efficiency by using NIC with four modules.

We verified the proposed structures by experiments on bus redundancy for communication line reliability, module redundancy for confirming communication module reliability, and switch redundancy for switch HUB reliability. All error-recovery rates are 100% - all in the situational cases when communication circuits are cut during the communication between slaves and masters, when the uses of modules are stopped in the same conditions, and when the power supplies to switches are cut. The fault detection time is also less than 1ms. For these reasons, we consider that the proposed systems show enough reliability to make the systems applied to railway signaling systems.

Acknowledgements

The authors would like to acknowledge the counsel and discussion concerning reliable networking provided by Professors Kyung-Chang Lee (Pukyung National Univ.) and Suk Lee (Pusan National Univ.), in improving the quality of this paper. These Professors and Ji-Hun Park, who is taking a Ph. D course at Pusan National Univ., have given significant contributions to the experimentation with the Ethernet-based network algorithm.

References

[1] Hideo Nakamura, “Development of Computerized Interlocking SMILENET”, RTRI Report, 1986.

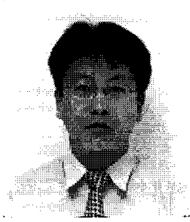
[2] Nishida Shigenobu and etc., “Replacement of Tokaido Shinkansen Signaling System Providing Advanced Train Controls in the 21st Century”, KYOSAN CIRCULAR, Vol. 53, No. 2, 2002.

[3] IEEE standard 802.3, Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, 2000.

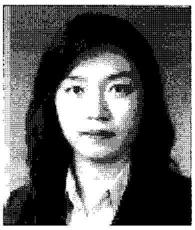
[4] G. Kaplan, “Ethernet’s winning ways”, *IEEE spectrum*, vol. 38, no. 1, pp. 113-115, 2001.

[5] W. Stalling, *Local and Metropolitan Area Networks*,

6th Ed. Macmillan Publishing Company, 2000.
[6] B. Y. Choi, S. Song, N. Birch and J. Huang, "Probabilistic approach to switched Ethernet for real-time control applications", in *Proc. Seventh International Conference on Real-Time Computing Systems and Applications*, 2000, pp. 384-388.
[7] K. C. Lee and S. Lee, "Performance Evaluation of Switched Ethernet for Real-time Industrial Communications", *Computer Standards & Interfaces*, Vol. 24, No. 5, pp. 411-423, Nov. 2002.



Jong-Gyu Hwang
He received his B.S., M.S. degrees and Ph. D. in Electrical Engineering from Konkuk University and Electrical and Computer Engineering in Hanyang University 1994, 1996 and 2005, respectively. As of 1995, he has been a senior researcher with the Train Control System Research Team of the Korea Railroad Research Institute (KRRI). His research interests are in the areas of railway signaling, protocol engineering, communication and computer network technology.



Hyun-Jeong Jo
Hyun-Jeong Jo received her B.S. degree from the Hankuk Aviation University, Goyang, Gyonggi-do, Korea, in 2003. She worked towards her M.S. degree at the Gwangju Institute of Science and Technology (GIST), Gwangju, Korea, from 2003 to 2005. Since December 2005, she has been engaged with the Train Control System Research Team of the Korea Railroad Research Institute (KRRI).