

Immunity Test of IP Devices against Repetitive Impulsive Noise

Naomichi Nakamura^{#1}, and Ryuichi Kobayashi^{#2}

[#]NTT Energy and Environment Systems Laboratories

9-11, Midori-cho 3-chome Musashino-shi, Tokyo 180-8585 Japan

¹nakamura.naomichi@lab.ntt.co.jp

²kobayashi.ryuichi@lab.ntt.co.jp

Abstract— The use of IP services is spreading widely with the advent of Internet technologies. These services, especially real-time services such as IP-TV, strongly require sufficient Quality of Service (QoS), and they are sensitive to impulsive noise. On the other hand, on user premises, impulsive noise occurs when home electric/electronic appliances are operated, e.g., when switches are turned on and off. Therefore, electromagnetic compatibility (EMC) problems may occur, and test methods based on QoS need to be studied. In this study, we investigated an immunity test of IP networks focusing on Ethernet frames. First, a simple simulation of the interaction between impulsive noise and Ethernet frames was carried out. Then an immunity test based on IEC standards was carried out, and the results were compared with the simulated ones. The simulation results agreed well with the measured results, which demonstrates the validity of the simulation method. Finally, by examining different frame loss rates, we found it is possible to determine the place where the error occurs.

Keyword: - repetitive impulsive noise, IP devices, immunity, QoS.

I. INTRODUCTION

With the advent of telecommunication technologies, a lot of telecommunication services are provided by IP networks. These services require that Quality of Service (QoS) be controlled in order to ensure their reliability [1]. Real-time services, such as IP-TV or high-quality Voice over IP, are one of the representative services based on IP technology, and they require high quality performance. Furthermore, these services do not require re-transmission of data because the delay of data is restricted to ensure its quality.

However, there are a lot of electric/electronic devices installed in customer premises, and they may be connected to the networks. These apparatuses may create impulsive noise when they operate or when they are turned on or off. In fact, quality degradation of IP-TV services that is caused by repetitive impulsive noise has been reported by several telecommunication operators [2]. Therefore, new electromagnetic compatibility (EMC) problems due to impulsive noise may occur in telecommunication networks.

In current immunity tests, however, criteria for transient phenomena, such as the Electrical Fast Transient / Burst test, permit performance degradation of the equipment under test (EUT) during the test [3].

Moreover, the relationship between EMC performance and the quality of IP service has not yet been studied. This paper evaluates the immunity test results of IP devices against

repetitive impulsive noise [4]. We focused on a frame loss of the Ethernet to evaluate its immunity to impulsive noise [4-5]. First, the frame loss rate of the Ethernet was calculated by using a simple simulation method, and the relationship between the frame loss rate and the repetitive frequency of the impulsive noise was examined [5]. Second, in order to confirm this relationship, an immunity test of IP devices was carried out, and the results were compared with the simulation results. Finally, by investigating the Ethernet frame loss rate, we clarify the EMC problems that occurred in the IP network.

II. SIMULATION

A. Method for evaluating frame loss against repetitive impulsive noise

Real-time services are being provided over the Ethernet along with the wide spread use of IP networks. The QoS of these services is evaluated by using characteristics of the Ethernet, especially the frame loss. Moreover, most IP devices have Ethernet ports to provide these services. Thus, we focused on the Ethernet frame loss instead of the bit error rate (BER), which is usually used to evaluate the quality of digital transmission. The benefits of choosing the Ethernet frame loss is that it makes it easy to evaluate the immunity performance of IP devices and to connect these results with QoS results.

B. Outline of Ethernet

In an Ethernet, data are transmitted by Ethernet frames that consist of a header, the data, and a frame check sequence (FCS) field. IP devices transmit the frames in accordance with the address information in the header field. When the IP device receives the frame, it starts to check for errors in the Ethernet frame according to cyclic redundancy check (CRC) information in the FCS field. When a CRC error in a frame is detected by the IP device, the frame is discarded by the device and is not transmitted again.

C. Simulation conditions

To evaluate the relationship between frame loss and repetitive impulsive noise, we carried out a simple simulation. An overview of the simulation is shown in fig. 1. First, the frame and the repetitive impulsive noise were simplified as rectangle-shaped pulses. The lengths of the pulses were the same as the duration of the signals.

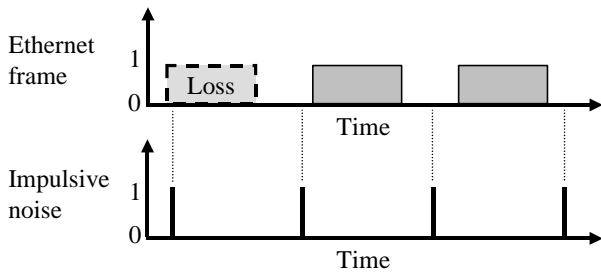


Figure 1 Ethernet frame and impulsive noise model

Table 1 Impulsive noise and Ethernet frame conditions

Impulsive noise conditions		Frame conditions		
Voltage Level [kV]	Repetitive frequency [kHz]	Frame length [byte]	Gap time [μ s]	No. of Packets
1	1, 3, 6, 9, 12, 15, 18	64	58	158000
		512	470	20000
		1024	940	9800
		1514	1380	6700

Then, we assumed that the Ethernet frame loss occurred when the impulsive noise overlapped the frame; i.e., we assumed 100% losses and evaluated the maximum frame loss during the time period. The time interval for calculating the frame loss was set to be the same as the Ethernet transmission period, and the calculation time was 10 s.

The simulation conditions are given in Table 1. In this study, the 100 Base-TX [6] Ethernet standard was evaluated. The interval was set at 8 ns instead of 10 ns because the 100 Base-TX standard uses a transformation called 4B5B at 100 Mbps. As shown in the table, the lengths of the Ethernet frame were set to be 64 bytes, 512 bytes, 1024 bytes, and 1514 bytes. The frame gap of each frame length was determined to be 58 μ s, 470 μ s, 940 μ s, and 1380 μ s respectively, in order to achieve 8 Mbps transmission. The repetitive frequency of the impulsive noise was changed from 1 kHz to 18 kHz.

The Ethernet frame loss rate was defined by the following equation.

$$F_{Loss} = \{1 - (F_{receive} / F_{transmission})\} \times 100, \quad (1)$$

where $F_{receive}$ and $F_{transmission}$ are the numbers of received and transmitted frames, respectively.

D. Results of Simulation

Fig. 2 plots the simulation results of each frame length vs. the repetitive frequency of the noise. The horizontal axis is the repetitive frequency, and the vertical axis is the frame loss rate calculated by eq. (1). From this figure, we can see that the Ethernet frame loss rate increases as the Ethernet frame length increases. Moreover, the frame loss rate increases when the repetitive frequency increases. In real situations, the frame length in the network is not fixed, and therefore, it has a distribution.

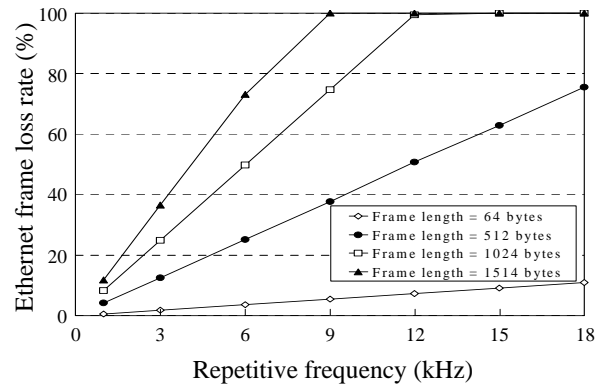
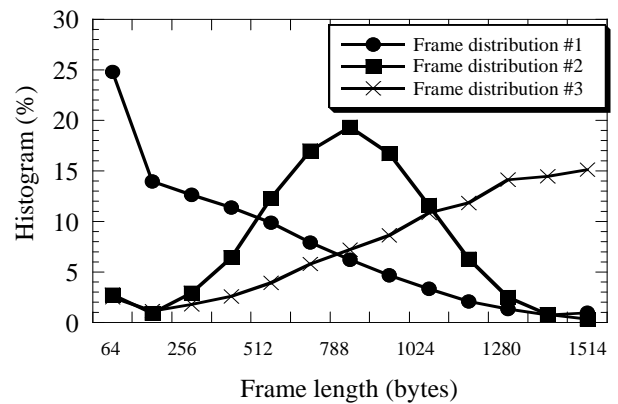
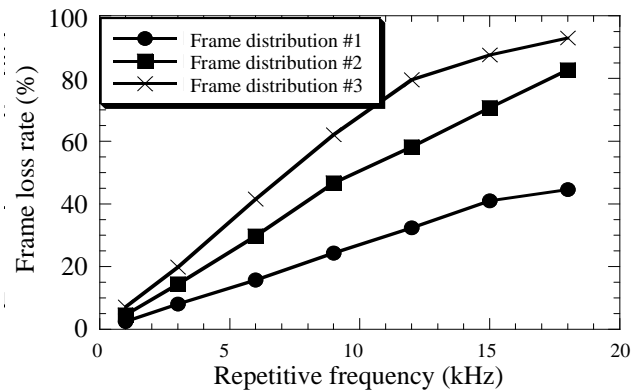


Figure 2 Simulation results



(a) Distribution of frame lengths



(b) Repetitive frequency of repetitive impulsive noise vs. frame loss

Figure 3 Simulation results for various frame distributions

Fig. 3 shows the simulation results when there are different frame length distributions. Fig. 3 (a) shows the distributions of frames. We assumed three distributions: distribution #1 was mainly composed of short frame lengths; #2 was primarily composed of medium length frames, and in distribution #3, the majority of the frame lengths were longer than the others. The simulation results are given in fig. 3 (b).

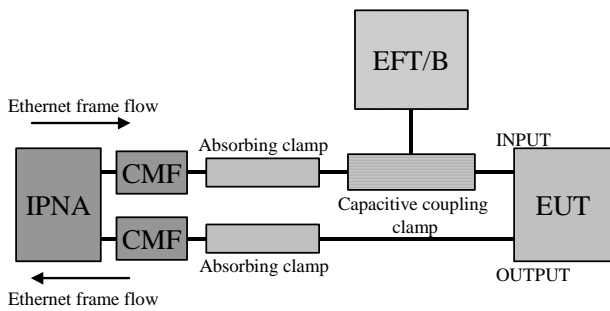


Figure 4 Immunity test setup

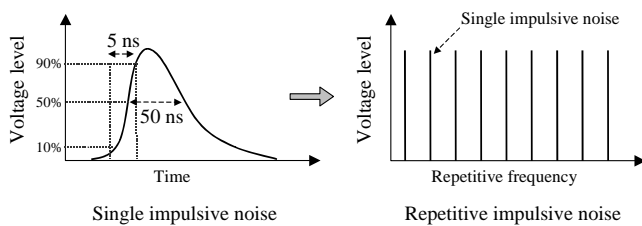


Figure 5 Configuration of the repetitive impulsive noise

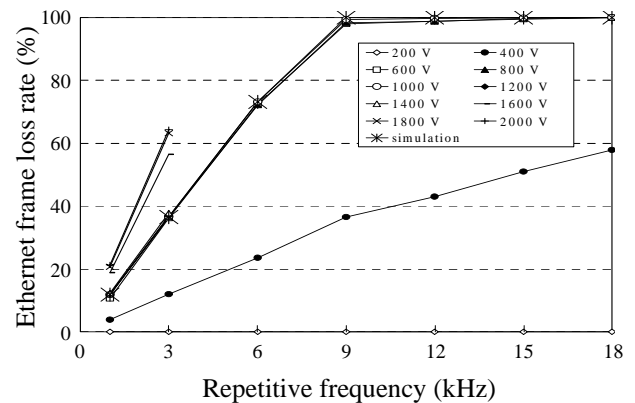
As shown in this figure, the frame loss rate of the shorter frame length distribution is also smaller than that of the long frame length distribution. From the results of figs. 2 and 3, therefore, shorter frames are more resistant to repetitive impulsive noise than longer ones.

III. MEASUREMENT

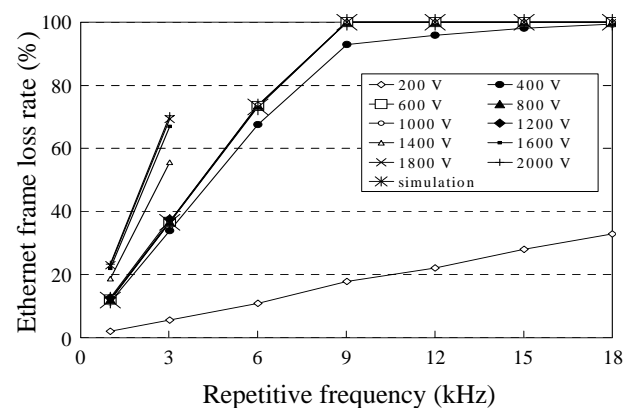
A. Measurement setup

To confirm the results of simulation, immunity tests against repetitive impulsive noise were carried out. The test setup is illustrated in fig. 4. The test was based on the electrical fast transient/burst (EFT/B) test defined by IEC61000-4-4 [5]. The applied impulsive noise was produced by an EFT/B generator and to a LAN cable by a capacitive coupling clamp. The configuration of the applied signal is given in fig. 5. We made the repetitive impulsive noise using single impulsive noise defined by IEC61000-4-4. An IP network analyzer (IPNA) was used to transmit and receive the Ethernet frames without retransmission. Common mode noise filters were used to protect the IPNA against the applied impulsive noise. The rate of Ethernet frame loss was obtained by the IPNA by using eq. (1).

In the test, two switching hubs were used as EUTs. The repetitive frequency of the repetitive impulsive noise was varied in a frequency range from 1 kHz to 18 kHz. The voltage level of the noise was varied from 200 V to 2000 V in 200-V steps. Due to the limits of the generator, the repetitive frequencies of 1 kHz and 3 kHz were only tested in the voltage range above 1200 V. The frame length and frame gap time were set at 1514 bytes and 1380 μ s, respectively, because the worst case should be evaluated in accordance with the simulation results. The transmitted number of Ethernet frames was 6700.



(a) Results of the test in HUB-A



(b) Results of the HUB-B

Figure 6 Immunity test results of two switching HUB

B. Results of the test

Fig. 6 (a) and (b) plots the test results of HUB-A and HUB-B, respectively. The horizontal axis is the repetitive frequency of the impulsive noise, and the vertical axis is the frame loss rate given by eq. (1). Compared with the same injection voltage, the loss rates generated in HUB-A and HUB-B increase when the repetitive frequency increases. Moreover, as the voltage level increases, the frame loss rate nearly corresponds to the simulation results until reaching the voltage level of 1200 V. This means that the assumption of the simulation, i.e., that loss occurs when the frame and the noise overlap, actually occurred in the real test. Thus, the simulation method is valid for evaluating Ethernet frames. Furthermore, comparing fig. 6 (a) and (b), the results of HUB-B quickly approach the simulation values. The test results indicate that the immunity level of HUB-A is stronger than that of HUB-B. However, if the level of the applied voltage exceeds 1200 V, the frame loss rate also exceeds the simulation results.

To confirm this phenomenon, the frame loss was plotted along with the variation of the voltage. The results are presented in fig. 7. These graphs were plotted based on data from fig. 6 using a repetitive frequency of 1 kHz.

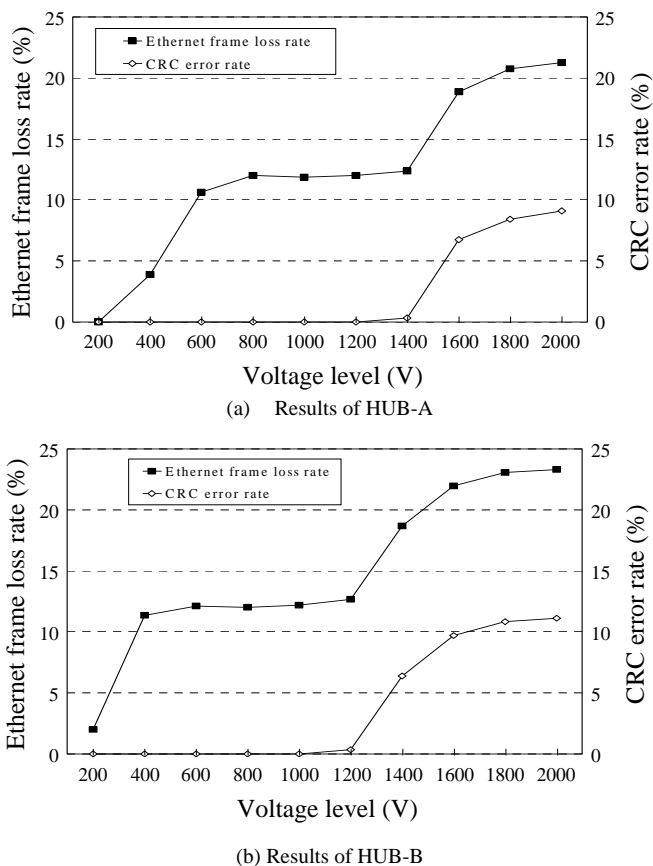


Figure 7 Relationship between applied voltage level and Ethernet frame loss

In these figures, the rectangles indicate the Ethernet frame loss rate, and the triangles represent the CRC error rate, which is given by the following equation.

$$CRC_{error} = \{1 - (CRC_{detect} / F_{transmission})\} \times 100 \quad (2)$$

where CRC_{detect} is the number of CRC errors detected by the IPNA.

As a result, the frame loss for each device was saturated below 1200 V, and no CRC error was observed in fig. 7 (a) or (b). However, above the voltage level of 1400 V, the frame loss rate increased, and the CRC error rate also rose. As we mentioned in section II-B, the IPNA cannot detect a CRC error, because the frame is discarded by the IP device and is not transmitted to IPNA again when a CRC error is detected by the device. By taking this point into account, it is presumed that the increase in the frame loss rate above 1400 V occurred inside the EUT or in its output port. This means that a correct Ethernet signal cannot be output from the EUT due to the malfunction that occurred inside it, or that the output signal is affected by the repetitive impulsive noise that passes through the EUT. On the other hand, the frame loss occurred at the input port of the EUT when the applied voltage level was below 1200 V. These results in fig. 7 indicate that by taking

the occurrence of the frame loss into consideration, the place that creates an error can be distinguished, e.g., in fig. 7 (a), the frame error may have occurred at the Ethernet input port of the device below 1200 V. On the other hand, a frame loss above 1200 V may occur inside the EUT or the output port (or connected cable) of the EUT because the applied repetitive impulsive noise may pass through the devices.

IV. CONCLUSION

In this paper, we examined the relationship between Ethernet frames and repetitive impulsive noise. The purpose of this study was to fundamentally consider the immunity test against impulsive noise based on the quality of services. As a result of this study, the following points were clarified.

- 1) A simple simulation method was valid for evaluating Ethernet frame loss. The simulation results indicated the maximum frame loss regarding interaction between the signal and the noise at the input port of the device.
- 2) A short Ethernet frame length showed good immunity against repetitive impulsive noise. This means that the shorter frame length was effective for transmitting data without re-transmission.
- 3) The immunity test results indicate that by taking the frame loss of the Ethernet and CRC errors into account, it is possible to determine the location where an error of the frame occurs.

In the future, we plan to work on clarifying and classifying the relationship between the frame loss and BER, and of the relationship between the immunity performance and the quality of service.

ACKNOWLEDGMENT

The authors would like to thank Mr. Kimihiro Tajima for his helpful technical advice.

REFERENCES

- [1] J. Song, et al., "Overview of ITU-T NGN QoS Control", IEEE Communications Magazine, Vol. 45, Issue. 9, pp. 116-123, 2007.
- [2] ITU-T K.74, "EMC, Resistibility and Safety requirements for home network devices", Appendix II, 09/2008.
- [3] IEC61000-4-4, "Testing and measurement techniques Electrical fast transient/burst immunity test", 1995.
- [4] R. Kobayashi, N. Nakamura, T. Suzuki, H. Kawano, and Y. Akiyama, "IP Broadband Services and EMC in the User Environment", NTT Technical Review, Vol. 5, No. 20, pp. 1-7, 2007.
- [5] N. Nakamura, et al., "Immunity test of IP device against impulsive noises", 2008 IEICE general conf. B-4-5, 2008 (in Japanese).
- [6] IEEE802.3u, "MAC Parameters, Physical Layer, Medium Attachment Units and Repeater for 100Mb/s Operation", 1995.