Secure Multimedia Transmission in IPv6 Wireless Networks

Haeyong Kim, Yongho Seok and Yanghee Choi
School of Computer Science and Engineering
Seoul National University
{hykim, yhseok, yhchoi}@mmlab.snu.ac.kr

***Abstract*— The security is very important during transmission of data in wireless network. Bit errors frequently occur in wireless network, which take critical data losses as encrypted data is decrypted consequently. The relations was researched between bit errors and serviced quality after decryption about several encryption algorithms supported by IPv6. RC4 shows the higher PSNR than DES in CBC mode and AES in CBC mode when JPEG and MPEG multimedia data is transmitted.**

***Index Terms*— secure transmission, encryption, wireless network, JPEG, MPEG.**

I. Introduction

The security is very important during transmission of multimedia data used commercially in wireless network. The most popular method to secure multimedia data is to treat the whole data as a binary file and encrypt it using encryption algorithms of IPsec defined IPv6. However, an encryption algorithm such as DES (Data Encryption Standard) is very complicated and require large amount of computation. In related work of [1] and [2], they proposed a fast encryption algorithm to process the vast amount of data generated by multimedia application.

It was considered in this paper that an effect on user level quality caused by bit errors in wireless network when multimedia data is encoded and encrypted. Because the feature of encryption algorithms, an enrypted block is currupted completely when more than one bit error occurs. When multimedia data such as an image or a video is decrypted in receiver of wireless network, several encryption algorithms supported by IPsec show the different performance. PSNR is used as index of user-level quality in the error-rate range from 10^{-7} to 10^{-4}. Each simulation result for JPEG and MPEG encoding data is in the section 2, and conclusion is in the section 3.

II. Encryption Algorithms in Wireless Network

When the multimedia data is transmitted, it is encoded for reducing required bandwidth and encrypted for security in transmission. The following Fig. 1 is an example of our simulation.

First, we encode the original image and movie for making the JPEG image and MPEG video file. Second, we consider four encryption methods which are RC4, DES in CBC mode, AES in CBC mode and Non-encryption. Third, since bit error is happened in Transmission process of wireless network, it is modeled by using Poisson process. Lastly, we calculate the PSNR(Peak-Signal to Noise Ratio) after decryption and decoding the transmitted data.

This work was supported in part by the Brain Korea 21 project of Ministry of Education and in part by the National Research Laboratory project of Ministry of Science and Technology, 2004, Korea.

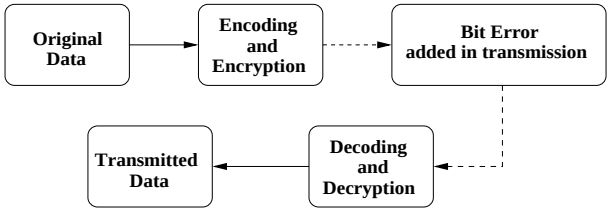

Fig. 1. A typical transmission of multimedia data on wireless network

A. JPEG Test

It will be discussed how the PSNR is changed by the use of each of the four encryption methods mentioned above and by the use of JPEG encoding when bit errors occur during transmission.

- When decoding or decryption fails because of added bit errors, PSNR is considered to be zero.
- In Fig. 3, the MAX is the PSNR when no bit errors were added. Simply, it is the PSNR when data losses occur with only JPEG encoding.

The result shows that PSNR is proportional to $\log(\frac{1}{BitErrorRate})$ when JPEG encoding is not used. When JPEG encoding is used, bit errors have a greater effect so that the PSNR lowers rapidly as the bit error rate increases. This is logical because JPEG encoding is a loss compaction method. If the bit error rate is more than 10^{-5} when JPEG encoding is used, PSNR is less than 8. That is, the original data corrupts totally regardless of the encryption method. If the bit error rate is lower, there are PSNR differences among the four types of encryption. Regardless of whether JPEG encoding was used, Non-encryption and RC4 encryption algorithm have the highest PSNR followed by DES in CBC mode, AES in CBC mode has the lowest PSNR.

B. MPEG Test

Similar to JPEG encoding, MPEG video is changed into a set of images by decoding MPEG video. The PSNR is then

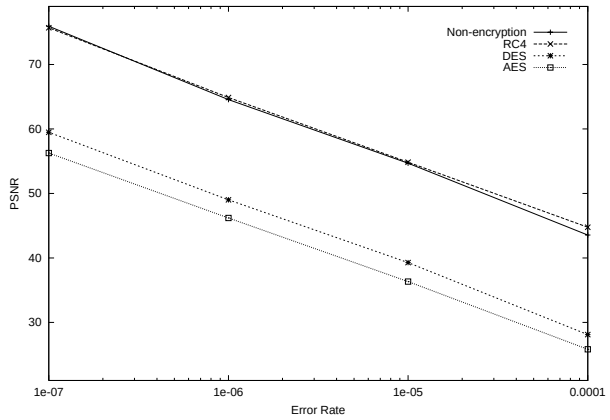

Fig. 2. In case that JPEG encoding is not used (Transmitted File size : 10,951,200 byte)

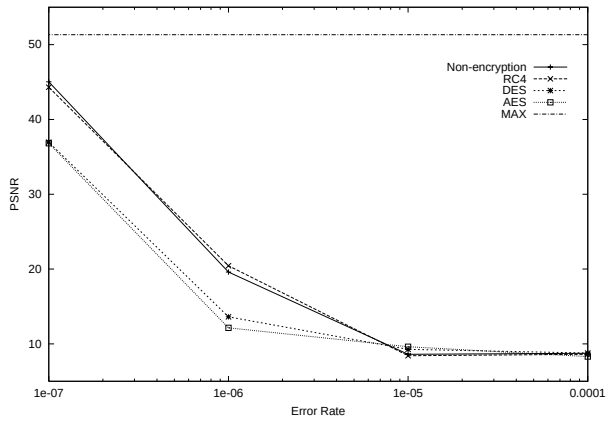

Fig. 3. In case that JPEG encoding is used (Transmitted File size : 666,956 byte, compression ratio : 6.09%)

calculated between the original set of images and decoded set of images. Then it is examined to see which type of encryption has the highest PSNR with the same bit error rate.

- The original video file has 150 frames (304,128 bytes/frame), which is encoded by MPEG2 algorithms (GOP = 12).
- When a decoding or a decryption fails because of added bit errors, PSNR is considered to be zero.
- In Fig. 4, the MAX is the PSNR when no bit errors were added. Simply, it is the PSNR when data losses occur with only MPEG encoding.

In the MPEG encoding test, the results obtained are similar to the JPEG encoding test. Non-encryption and RC4 encryption algorithm have the highest PSNR followed by DES in CBC mode. AES in CBC mode has the lowest PSNR. The notable point is that, as the bit error rate increases, the PSNR decreases more slowly with MPEG encoding than when no encoding is used. [Fig. 2] This is because MPEG encoding associates the current frame with some of previous and following frames. So although current frame is partially

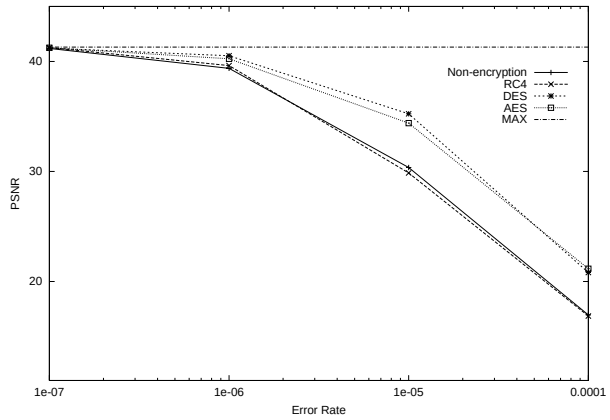

Fig. 4. In case that MPEG2 encoding is used

corrupted, it can be recovered from some of previous and following frames.

III. CONCLUSION

From above test results, RC4 is the best encryption algorithm against bit errors with JPEG and MPEG encoding data. This result is because RC4 is a stream encryption algorithm.

In the case of DES algorithm (64bits encryption algorithm), if more than one bit error is inserted to 64 bits encrypted data it matches 32.06 bits (about 50.09%) on the average with original data when decrypted. Because the probability is 50% that match two random 64bits data, the 50.09% match result is not concluded that is over 50% when use a 95% significance probability. That is encrypted data by DES algorithm corrupts totally with more than one bit error. Similarly, in the case of AES algorithm (128bits encryption algorithm), more than one bit error makes the whole 128 bits data corrupt. However, encrypted data by RC4 algorithm has only one bit error if one bit error is inserted because RC4 is a stream encryption algorithm. So result is that using RC4 encryption is almost the same as using non-encryption.

In an encryption test with JPEG encoding, more than one bit error in a block (unit of encryption file size) corrupts 64bits data in DES algorithm and 128bits data in AES algorithm. So the PSNR when using DES algorithm is better than when using AES algorithm. In the case of MPEG encoding, however, the existence of an error bit is more important than the amount of data loss (64bits or 128bits) because the current frame is associated with previous and following frames so the PSNR when using DES algorithm and when using AES algorithm are almost the same in the MPEG encoding test.

In conclusion, the best encryption algorithm is RC4 (one of streaming encryption algorithm) during real-time data transmission in a wireless network

REFERENCES

[1] Ali Saman Tosun, Wu-chi Feng, “Lightweight Security Mechanisms for Wireless Video Transmission”, in Proceedings of the IEEE International Conference on Information Technology: Coding and Computing 2001, Las Vegas, Nevada, April 2001.

[2] Bharat Bhargava, Changgui Shi and Sheng-Yih Wang, “MPEG Video Encryption Algorithms”, West Lafayette, IN 47907, USA, August 2002.