INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT
Int. J. Network Mgmt 2001; **11**:147–159 (DOI: 10.1002/nem.398)

Security-enhanced packet video with dynamic multicast throughput adjustment

By Han-Chieh Chao, T. Y. Wu and Jiann-Liang Chen*

In recent years, the Internet population has increased at an explosive rate. Many problems exist because Internet packets are not encrypted and the bandwidth is not large enough. In this research, we propose a datagram encryption technique and dynamic bandwidth throughput adjustment. Security is enhanced using secret keys selected from a Key-Database. Not only is a double encryption tunnel offered but also the whole plaintext can be encrypted more than one key depending on the encryption block size chosen. Copyright © 2001 John Wiley & Sons, Ltd.

Introduction

Video multicast distribution is an important component of many existing and future networked services. Today's Internet lacks adequate support for quality of service (QoS) assurance, which makes the transmission of real-time traffic (such as video) challenging.[1] Many of these problems exist because Internet packets are not encrypted and bandwidth is not large enough. An Internet without a security infrastructure in place is vulnerable to several types of attack. Internet use continues to increase dramatically along with the variety of data exchanged over computer networks.[2,3]

Videoconferencing is becoming part of distributed systems. Many distributed applications require information exchanges over insecure public channels. Private exchanges require protection from eavesdroppers. Secure information exchanges are a necessity in distributed systems. Encryption and decryption provide the basic technology for building secure systems. There are two encryption methods: secret key encryption and public key encryption. The decryption available from currently well-known public key schemes is slower than that in secret key schemes. Under security systems, a single key is used for both encryption and decryption and only authorized users possess this key.[4] We present a security-enhanced secret key encryption method using a Key-Database and traditional encryption. This system encrypts plaintext using random keys selected from a Key-Database. The brute-force approach can then be avoided for it is too time consuming.

Who handles retransmission and how retransmissions are processed are key distinguishing factors among reliable multicast transport protocols.

At the same time, we try to avoid overburdening the sender with control traffic and retransmission duties. Who handles retransmission, and how retransmissions are processed are key distinguishing factors among reliable multicast transport protocols. The source is ultimately responsible for retransmissions, but that doesn't necessarily mean that the source must be directly involved in each

Han-Chieh Chao, T. Y. Wu and Jiann-Liang Chen teach at the National Dong Hwa University, Hualien, Taiwan, ROC.

**Correspondence to: Dr. Han-Chieh Chao, Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan, ROC.*

Contract/grant sponsor: National Science Council of Taiwan; Contract/grant number: NSC 89-2119-E-259-002.

retransmission. Most of the previous approaches support real-time video transmissions in integrated services networks that rely on traditional preventive congestion control. Feedback control mechanisms are already used in the Internet to control non-real-time traffic sources. Feedback mechanisms for video sources have also been proposed for networks with variable capacity channels such as the Internet. Using multicast transmissions can reduce the datagram flow within WAN.[5–7] Many early congestion control methods involved adjusting the video quality and data rates over a relatively wider range. Real-time video and IP/TV adjust the bit rate to change the frame encoding to comply with the bandwidth. Traditional methods generate low-quality images that are sent to all subscribers regardless of whether their network nodes have reception congestion or not. The proposed method will only send low-quality encoded images to the nodes that are actually congested. The host server load is thus reduced since it is not necessary to regenerate the entire picture. The picture frames will drop out according to the priority assigned by the host at the beginning. The Key-Database encryption method and frame priority estimation are processed at the same time. The multicast router then controls the bandwidth accordingly.

The paper is organized as follows. The proposed security enhancement with Key-Database is described in the next section. This system contains the International Data Encryption Algorithm (IDEA) and Data Encryption Standard (DES) conventional encryption methods. The Key-Database enhances security using IDEA and improves the tunnel topology. The proposed dynamic throughput adjustment scheme is introduced in the third section. This scheme begins by considering multicast videoconference throughput adjustment over the Internet. The major issue is multicasting over the Internet. The question then arises about videoconference standard H.263. The main objective is dynamic throughput adjustment. In the following section, the experimental results are listed. Conclusion is presented in the final section.

Security Enhanced with Key-Database

Any cryptographic primitive, such as a block cipher or a digital signature algorithm, can be thought of in two very different ways. IDEA is a product block cipher that resists all current publicly known forms of crypto-analysis. We describe a technique for enhancing the IDEA symmetric cipher using Key-Database. There are several conventional encryption algorithms available over secure network systems. IDEA cryptography was selected from several existing security algorithms. Table 1 compares several cryptographic systems that are available currently. IDEA has several important advantages. Because encryption algorithms can be used over an open source, they are better than other conventional encryption algorithms.

Compared to public-key encryption schemes, RSA, the structure of encryption algorithms is very complex. It is very difficult to explain RSA or similar algorithms in details. We propose using conventional encryption over videoconference, because usually more than one user will join the videoconference. If a datagram must be sent to newly joined users, public-key encryption is used for every user of the datagram. When there are

	DES	IDEA	RC5	Skipjack
Designer	NSA	Lai, Massev	Ron Rivest	NSA
Development	1977	1992	1994	1993
Data (bits)	64	64	64	64
Encrypted key	56	128	Variable	80
Round number	16	8	Variable	32
Algorithm (open source)	No	Yes	Yes	No

Table 1. Comparison of several conventional encryption algorithms

many participants, using a nontraditional scheme, the datagram must be encrypted as many times as the total participant number. Conventional encryption only needs to encrypt the datagram once. This definitely decreases the source-host load. The time required to encrypt a video file is approximately one quarter of the total video display time. That is, for a one-hour long, 15 minutes are needed to encrypt the entire file.

—Key-Database—

A Key-Database scheme is presented to enhance IDEA encryption algorithms without altering the original algorithms. The original IDEA encryption algorithm encrypts datagrams using one key. When the ciphertext flows from the source to a destination, it is vulnerable to an interception. An unauthorized party can capture the encrypted data in a network and use any method, such as the brute-force approach, to decipher the encrypted text. On average, half of all possible keys must be tried to achieve a brute force decryption. Table 2 shows how much time is involved for the various key sizes.

Table 2 shows the results of a 56-bit key size with 10.01 hours for decryption. The required cost and time is substantial. Although such a scheme, with a long key, presents formidable crypto-analysis difficulties, it can be broken with sufficient ciphertext using known or probable plaintext sequences, or both. The **one-time pad** is unbreakable. It produces a random output that bears no statistical relationship to the plaintext. Because the ciphertext contains no information about the plaintext, there is simply no way to break the code.

A Key-Database is proposed to replace the single-key scheme.[8] This approach involves using random keys from the Key-Database, producing a 65535 random key selection. The encryption process blocks are shown in Figure 1. Using our approach, the videoconference leader decides how often to replace a key from Key-Database. This conforms to the 'One–Time Pad'.

Figure 2 shows Key-Database IDEA encryption processes. We may recall that 4064 bits of plaintext is encrypted using the block size of 500 bits (approximately using 4064/500 = 8 different keys), it only takes 0.038 second to complete the whole video encoding and encryption. The proposed method has all of the advantages of IDEA. The time required for changing keys is only 0.935 μs obtained through experiments. This places little overhead on the whole process compared to 38 ms.

—Building a Double Encryption Tunnel—

This approach can also be applied to firewalls and virtual private networks (VPNs).[9] The IPSec supports these features and is mandatory for IPv6 and optional for Ipv4. In both cases, the security features are implemented as extension headers that follow the main IP header. The extension header for authentication is known as the authentication header (AH). The extension for encryption is known as the Encapsulating Security Payload (ESP) header. We would like to focus attention on the tunnel mode. The tunnel mode provides protection for the entire IP Packet. To achieve this, after the AH or ESP fields are added to the IP packet, the entire packet, plus the security field, is treated as the payload for the new 'outer' IP packet with a new outer IP header. The entire original, or inner, packet travels through a 'tunnel' from one point in an IP network to another. No routers along the way are able to examine the

Key size (bits)	Number of alternative keys	Time required at 1 encryption/μs	Time required at 10 M encryption/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\mu$ s = 35.8 s	2.15 ms
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\mu$ s = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\mu$ s = 5.4×10^{24} years	5.4×10^{18} years

Table 2. Average time required for an exhaustive key search