Protocol of Steganography in Streaming Media on VOIP Network Based on Variable Length Coding

Zhen Yang[1,2]
[1] Department of Electronic Engineering, Tsinghua University, Beijing, 100084, China
[2]National Laboratory for Information Science and Technology

Huaizhou Tao[1,2]
[1] Department of Electronic Engineering, Tsinghua University, Beijing, 100084, China
[2]National Laboratory for Information Science and Technology

Yongfeng Huang[1,2]
[1] Department of Electronic Engineering, Tsinghua University, Beijing, 100084, China
[2]National Laboratory for Information Science and Technology

Wanxia Yang[3]
[3]Engineering Institute of Gansu Agricultural University, Lanzhou, 730070,China

***Abstract* — Based on the three-layer model theory for steganography communication system, this paper designs a new steganography transmission protocol, to achieve a more effective frame structure, more reliable transmitting mechanism. Both text message dialogue and file transmission communication based on the proposed method are reliable while the performance is also corresponding improvement. The experimental results has proved theoretical prediction that the proposed protocol is able to achieve reliable and efficient steganography on VoIP network.**

Key Words- protocol, variable length coding, steganography, VoIP, Information hiding

I. INTRODUCTION

As an important branch of network information security, information hiding uses special algorithms to transmit information hidden in the carrier by passing the carrier to achieve covert communication. Steganography is a very important aspect of information hiding. In terms of hidden carrier, steganography can be divided into two categories: the first kind is based on static carriers such as image, audio, text, data and other documents; the second kind is a class of streaming media in real-time communication as a dynamic carrier. Compared with the former carrier, the latter one has many advantages: such as the amount of data, real-time interaction, no storage, and so on. Therefore, steganography using streaming media network protocol as the carrier is more secure. Existing methods of information hiding includes streaming audio, video encoding, and embedded storage network protocol type embedded, time-division-type embedding[1-2], and so on.

Xiao Bo[3] built a practical covert communication system for streaming media and made a 3-layer covert communication system model, which includes Steganographic Adaptation & Execution layer (SAE), Steganographic Transmission Management layer(STM), and Steganographic Information Application layer (SIA), and made more reliable retransmission mechanism for the LSB algorithm, using the STM layer data unit (STMDU) for the retransmission unit. The transmission bandwidth is also theoretically calculated. However, this system model has problems in the design, such as data embedding algorithm associated with the media, and system cannot handle packet loss caused by destruction of confidential information.

Variable length coding is widely used in image coding. By giving the symbol that has bigger probability a shorter code, variable length coding changes the length of code to compress information redundancy. Then, it has fully reversible encoding and decoding process, so it is also referred to as statistical encoding and lossless compression coding method. The most commonly used variable length coding method is Huffman coding[4], arithmetic coding and runlength coding. In addition, in Shannon's "A Mathematical Theory of Communication", his 1948 article introducing the field of information theory, Shannon proposed a new technique of data compression[5]. Then the method of that new technique was attributed to Fano, who later published it as a technical report. This method is called Shannon-Fano coding now. It’s a famous compressing coding method in the history[6].

For the problems exists before, combined with the new ideas, this paper proposed a new steganography protocol to support covert communication that offers multiple content delivery services such as text and documents. Also, by developing control mechanism and using variable length coding, the protocol can support reliable transmission and efficient handling of broken secret information caused by packet loss.

This paper is structured as follows: the second section describes the hidden protocol, the third section tells the implementation and tests, the fourth part is the conclusion.

II. MULTIMEDIA PROTOCOL OF STEGANOGRAPHY

In a practical covert communication system, the application layer SIA can have a variety of ideas. But interface between the SIA and STM must be set to static for part of the functions of SIA to ensure the complete implementation. STM itself also needs to have a series of mechanisms to ensure that they can achieve stable and reliable transmission.

As is described earlier, a steganography protocol can achieve transmitting different kinds of information, and even

Corresponding author: YANG Zhen(e-mail:eeyangzhen@gmail.com)

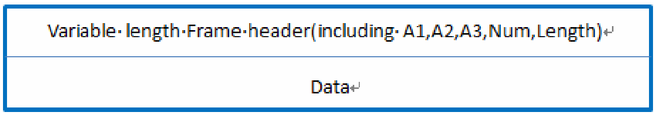
multimedia. This protocol corresponds to the SIA layer to provide service such as file transmitting and text transmitting. And it corresponds to the STM layer to solve problems caused by packet loss through mechanisms such as retransmission.

A. Protocol data unit description

Protocol data unit (PDU) consists of two parts: the header (control information) and data (secret message data). In the system, the data frame is STM and SAE data exchange format. After STM receives SIA level data, based on the agreement, STM will divide type of information, secret information, information integration and so on into frames. Then the transmitted data frame will be sent to SAE-by-layer. SAE layer will execute steganography to achieve the single frame in a packet. Steganography algorithms and the choice of steganography object data packet, are available through an external algorithm libraries and other means freedom of choice.

From the Fig 1 and TABLE 1, the frame structure shows the whole frame includes a variable length header and frame data. Generally speaking, frame header should be set as a certain length, such as 8bits or 16bits. However, to improve data bandwidth, variable length header can reduce the usage of header bandwidth.

The variable length header should express some items showed in the Fig 1 and TABLE 1,such as A1,A2,A3,Num and Length. If set them as fixed bits, their cost are showed in the TABLE 1. As is shown before, Huffman coding is a quite good compress coding method. Then, Shannon-Fano coding is also a choice. Through using these two methods, we can make the average header length shorter.



Variable· length·Frame·header(including· A1,A2,A3,Num,Length)↵

Data↵

Fig. 1. Frame Structure

TABLE I Details about every ITEM of frame

Items	Fixed Bits Cost	Function
A1	1	Type of Frame Content: 0 means Data Frame 1 means Ack Frame
A2	1	Type of Data: 0 means message data 1 means file data
A3	1	Type of frame in frame series: 0 means not the last frame of packet 1 means the last frame of packet
NUM	5	Number of Frame in packet （1~31）
Length	6	Length of Frame Data(1~40)
Data	40Byte	Secret Data

In actural operation, 1 bit for frame content type(A1), 1 bit for data type, 1 bit for whether current frame is the last frame of a packet, 5 bits for number in packet and 6 bits for byte length of frame data should be first calculated. With calculated A1,A2,A3,Num and Length, we uses compress coding to make the header. By the way, a packet means a time of transmitting with maximum data capacity of 31*40=1240bytes. With header and data prepared well, STM layer can send the STMDU to receiver.

In the part of receiver, when receiving a frame, the header should firstly be decoded to A1,A2,A3,Num and Length. Then receiver can achieve next steps.

B. Multimedia steganography

Because of the frame set above in 2.1, every layer has a chance to know if the frame is file or message. As file is quite different from message, different approach of transmitting should be made.

As is known to everyone, message data is usually short, light and convenient. And file data is often long, heavy and distribute in different SIADUs(SIA layer Data Unit). To some extent, if a piece of message seems to be a car, then similarly a file can be thought as a train. Lightweight message can be transmitted directly, but the heavy load of files needs to increase the SIA layer mechanism to control to achieve transmitting stability. A car can running on the ground directly, but a train's running must needs something else like rail. Then the system can have functional integrity.

As most files need to transmit for not only once, a file stream is necessity. Every time when transmitting a part of file, temp file in the receiver will increase by appending new coming data. Another problem is file has its own information, such as create time, file name and so on. File information is needed when system interactive with the receiver. Solution is write file information first in the SIADU(SIA Data Unit). If file information is shorter than 1240 bytes, then system will read some file stream data to fill the space left. After first series of frames' transmitting, receiver can get the file information and some content data of file. Some choose can be made using file information, such as whether agreeing to receive this file.

C. Control mechanism of frame transmitting

In order to maintain the accuracy and stability of the transmitting procedure, avoid packet loss and other network problems brought to the secret information transmission errors, the transmission control module in STM layer using the "waiting to confirm" control method. This control method is based on stop protocol. In brief, after the issue of a data frame, the sender part will wait for reply of confirm frame of receipt of the data frame, then issue the next data frame. If you haven't received confirmation frame, the sender part will resend the data frame. This method avoids the loss arising from the secret data loss and errors.

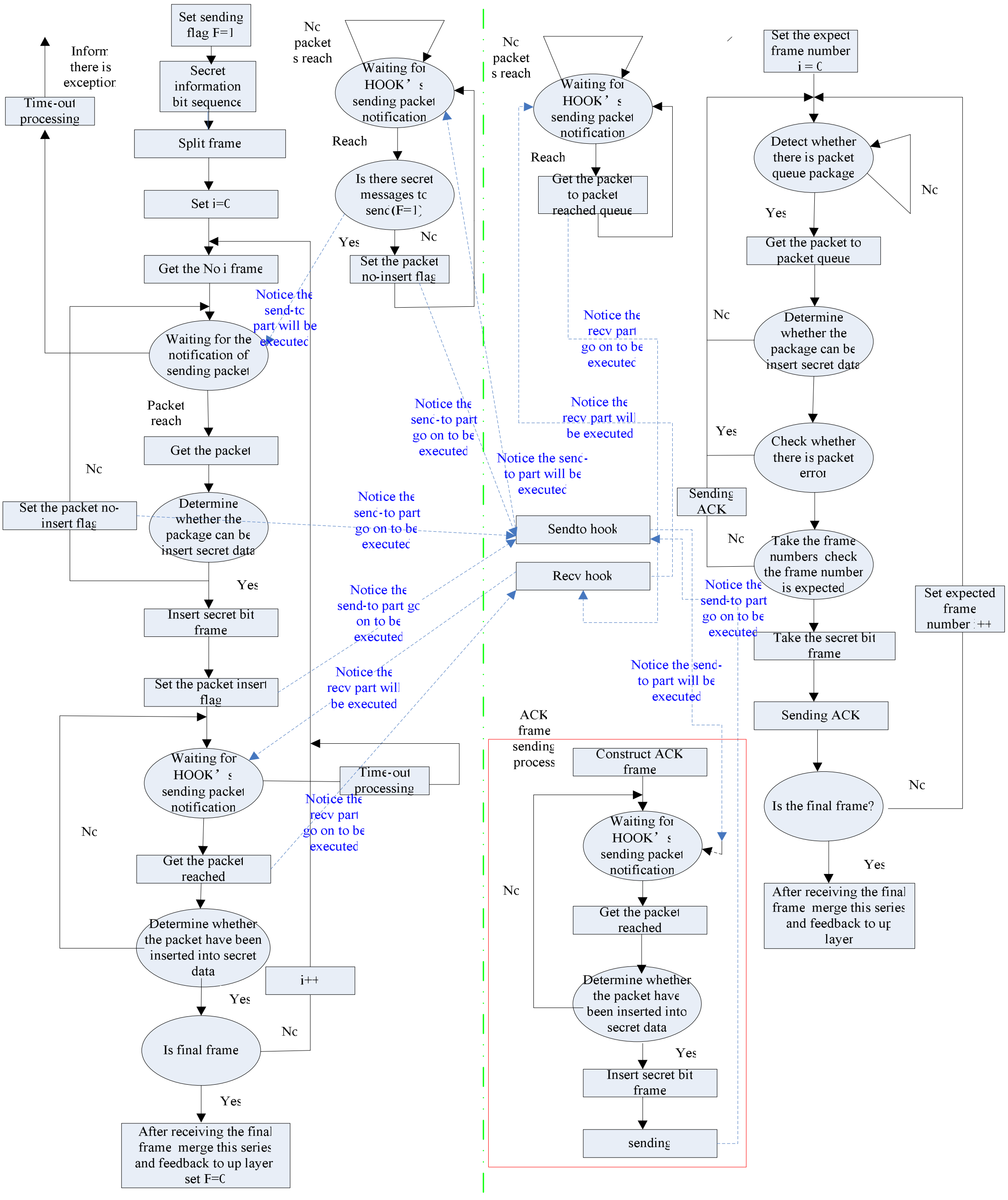
Transmission control module runs a specific process flow chart as shown in Fig 2.

III. A IMPLEMENTATION OF THE PROTOCOL AND TEST

Accordance with the above protocol and control mechanisms, this paper experiments with VoIP streaming media as the carrier to implement a VoIP-based audio streaming of steganography utility software.

There are some important points must be shown here in the software system. Firstly it is the compress coding method. Indeed if anyone wants to use variable length coding to reduce average length, then the probability of every condition must be calculated or the frequency must be counted.

To calculate the probability, we assume that any length of frame between 1 byte and 40 bytes has the same probability and any length of packet has same probability to appear. Then we think the data frame and acknowledge frame should be the same number in normal condition.



Set sending flag F=1
Secret information bit sequence
Split frame
Set i=C
Get the No i frame
Waiting for the notification of sending packet
Packet reach
Get the packet
Determine whether the package can be insert secret data
Set the packet no-insert flag
Yes
Nc
Insert secret bit frame
Set the packet insert flag
Waiting for HOOK's sending packet notification
Time-out processing
Get the packet reached
Determine whether the packet have been inserted into secret data
Nc
Yes
Is final frame
i++
Nc
Yes
After receiving the final frame merge this series and feedback to up layer set F=C
Inform there is exception
Time-out processing
Nc packets reach
Waiting for HOOK's sending packet notification
Reach
Is there secret messages to send (F=1)
Yes
Nc
Set the packet no-insert flag
Notice the send-to part will be executed
Notice the send-to part go on to be executed
Notice the send-to part go on to be executed
Notice the send-to part go on to be executed
Notice the recv part will be executed
Notice the recv part go on to be executed
Sendto hook
Recv hook
Notice the send-to part will be executed
Nc packets reach
Waiting for HOOK's sending packet notification
Reach
Get the packet to packet reached queue
Notice the recv part go on to be executed
Notice the recv part will be executed
Set the expect frame number i=C
Detect whether there is packet queue package
Nc
Yes
Get the packet to packet queue
Nc
Determine whether the package can be insert secret data
Yes
Check whether there is packet error
Sending ACK
Nc
Take the frame numbers check the frame number is expected
Notice the send-to part go on to be executed
Set expected frame number ++
Take the secret bit frame
Notice the send-to part will be executed
Sending ACK
Is the final frame?
Nc
Yes
After receiving the final frame merge this series and feedback to up layer
ACK frame sending process
Construct ACK frame
Waiting for HOOK's sending packet notification
Nc
Get the packet reached
Determine whether the packet have been inserted into secret data
Yes
Insert secret bit frame
sending

(a) secret bits sending process

(b) secret bits receiving process

Fig. 2. Control Machanism

Then we can use total probability formula to calculate probability. Total probability formula is shown below:

$$P(A_k)=\sum_{i=1}^{n} P(A_k|L=i)P(L=i)$$

Fig. 3. Total probability formula

In the formula, A_k means No.k frame appears. L means the frame number including in a packet.

Another problem is how to allocate the percentage of message data and file data in all data. We set the percentage a parameter α, that means the percentage of message data in all data. With a changing parameter α, we can all the conditions can be considered.

Secondly, an necessary process is implying the encoding of Huffman coding and Shannon-Fano coding. The former one uses bottom-up method and the latter one uses top-down method. Using C language, we imply the two algorithms in the software system.

Finally, with a GUI software on a simple design, the software achieve <10MB file and <1240B of message transmission.

Then we have done some experiments. At first, let's talk about the compress coding. With the probability calculated before, we have tested Huffman and Shannon-Fano coding. The bandwidth of frame header can be shown through average frame header length. Besides, the coding efficiency is another quite significant index. Average frame header length is shown in Fig 4. Coding efficiency is shown in Fig 5.

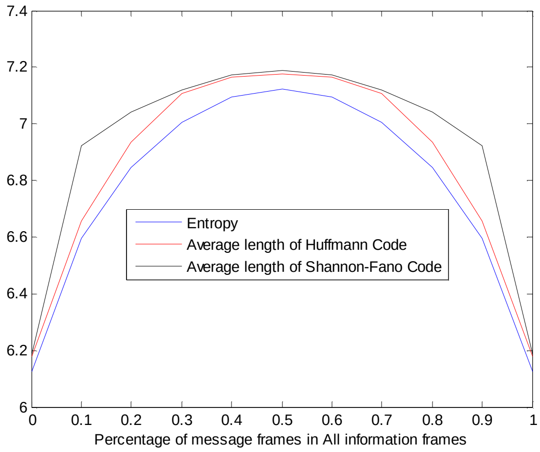


Fig. 4. Frame header Entropy and average length using Huffman Code and Shannon-Fano Code

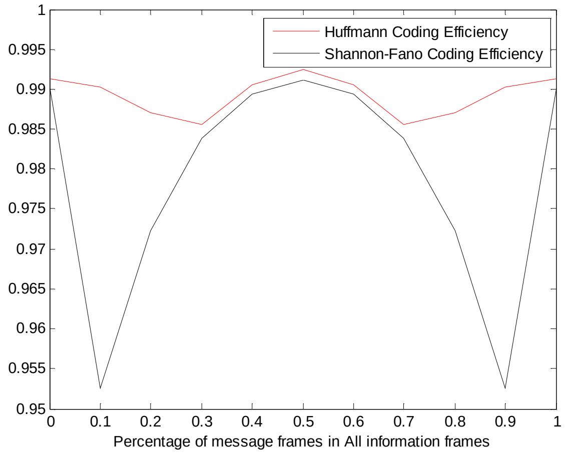


Fig. 5. Compress coding efficiency of frame header between Huffman and Shannon-Fano coding

From Fig 4 and Fig 5, we can see that during different α, Huffman Code is always shorter than Shannon-Fano Code length and is closer to the entropy. Then we get the coding efficiency of Huffman Code is higher than Shannon-Fano Code. Compared with fixed bits, Huffman code and Shanon-Fano code both reduce 14bits to 6 or 7bits. The decline is so obvious that our theoretical prediction is implied.

In data transmitting reliability experiments, we use three test circumstances. They are campus net to campus net, ADSL to ADSL and campus net to ADSL. Also we use message and different type of file data. The result is shown in Table 2.

About data transmitting correctness, a similar experiment has been done when environment is so bad that packet loss exists. When packet loss rate is 10%, error rate is 0%. When packet loss rate is 20%, error rate is 0%. The higher is packet loss rate, the longer time delays.The result is shown in Table 3.

TABLE II Error Rate Test in ThREE circumstances

circumstances	ADSL-ADSL		Campus-campus		ADSL-campus	
Transfer	Secret Data(Bytes)	Error Bits	Secret Data(Bytes)	Error Bits	Secret Data(Bytes)	Error Bits
Message	50000	0	50000	0	10000	0
doc	11377770	0	11377770	0	11377770	0
docx	11377770	0	11377770	0	11377770	0
exe	11377770	0	11377770	0	11377770	0
jpg	11377770	0	11377770	0	11377770	0
mp3	11377770	0	11377770	0	11377770	0
pdf	11377770	0	11377770	0	11377770	0
ppt	11377770	0	11377770	0	11377770	0
rar	11377770	0	11377770	0	11377770	0
txt	11377770	0	11377770	0	11377770	0

TABLE III Error Rate Test in packet loss circumstances

Packet Loss Rate	Data Amount Every Time	Times	Whole Data Amount	Error Rate
1/10	500Bytes	20	10000Bytes	0%
1/5	500Bytes	20	10000Bytes	0%

As is shown above, system can ensure reliable data transmitting.

IV. CONCLUSION

In the network environment of streaming media, we are able to use the proposed method to make covert communication for message dialogue communication and file transfer communication.

The proposed protocol can implement a steganography system with reliable transmitting and offer more data bandwidth through variable length coding of frame header. And that rate is practical. The protocol is against packet loss.

But the transmitting control mechanism should improve from stop protocol to sliding window protocol. Then the performance of whole system will be better.

REFERENCES

[1] Katzenbeisser Stefan, Petitcolas Fabien, Information hiding techniques for steganography and digital watermarking, Artech Print on Demand: 1999

[2] U.S. Department of Defense, Department of Defense Trusted Computer System Evaluation Criteria, DOD 5200, 28-STD, [2008-03-31]. http://csrc.nist.gov/publications/history

[3] Xiao Bo, Huang Yongfeng, Modeling and Optimizing of Information Hiding Communication System over Streaming Media. JOURNAL OF XIDIAN UNIVERSITY(NATURAL SCIENCE), 2008 , 35(3)

[4] DAVID A. HUFFMAN,A Method for the Construction of Minimum-Redundancy Codes, Proceedings of the I.R.E., sept 1952

[5] Shannon, C.E. (July 1948). "A Mathematical Theory of Communication". Bell System Technical Journal 27: 379–423.

[6] Fano, R.M. (1949). "The transmission of information". Technical Report No. 65 (Cambridge (Mass.), USA: Research Laboratory of Electronics at MIT).