A Model-Based Analysis of Secure Video Transmission Based on IPSec and IPv4

Quang-Dao Van, Anne Wei, Benoît Geller, and Gérard Dupeyrat

ABSTRACT—A promising solution to protect wired Internet networks is to use the Secure Internet Protocol (IPSec); however, this has some drawbacks, particularly on the quality of service (QoS). This paper aims at evaluating the video traffic QoS in terms of end-to-end delay and packet loss rate. Based on some basic assumptions, our analysis shows that the performance with IPSec is rapidly inferior to the IPv4 performance. We thus suggest adding some QoS parameters into IPSec in order to achieve a compromise between QoS and security.

Keywords—CBR video, IPSec, IPv4, QoS.

I. Introduction

As network threats including loss of privacy, loss of data integrity, identity spoofing, and denial-of-service happen daily, security is now considered a crucial issue. To face these different problems, we should distinguish between two types of security processing. The first one concerns conventional cryptography methods such as private and public key encryption and hash algorithms. This paper deals with the second type, represented by authentication techniques and securing network protocols. Unfortunately, security measurements burden network performance. In some cases, the Quality of Service (QoS) of multimedia is even completely degraded. For instance, in the case of video transmission, the end-to-end delay should not exceed 150 ms [1]; without any security measurement, a network with a capacity of 10 Mbps allows the transmission of several video traffics; contrarily, this paper shows that if the IPSec protocol is introduced into a network using typical routers [2], the end-to-end delay often exceeds 150 ms because of the security processing delay. Moreover, the "tunneling" solution limits an efficient use of the available bandwidth as all traffic coming into a tunnel cannot negotiate a specific bandwidth. As a result, it is difficult to ensure both security and QoS.

Different studies have already shown that the IPSec protocol degrades the QoS. For example, R. Barbieri and others [3] analyzed the influence of cryptographic schemes over voice traffic, while S. Ariga and others [4] studied the performance of different UDP/TCP streams. This paper concentrates on video traffic QoS in terms of end-to-end delay and loss rate when IPSec and classical IPv4 are applied. It first investigates the degradation on QoS caused by IPSec; then using an analytical model, this paper analyzes the performance of video traffic. The goal is to achieve a compromise between a minimum QoS and minimum security.

II. Protecting Video Traffic with IPSec

1. IPSec Using ESP in Tunnel Mode

We consider a configuration of IPSec [5] in tunnel mode using the Encapsulating Security Payload (ESP) [6]. In this case, the two extremities of the tunnel reside in the two security routers [2].

Unfortunately, the additional security measurements necessary to network security involve some loss of performance. This is due to some additional packet overhead and to an amount of security processing time.

2. IPSec Drawback Analysis

A. Additional Overhead

The additional overhead is caused by the new IPSec datagram encapsulating the original IP datagram. As depicted

Manuscript received Oct. 13, 2004; revised Feb. 10, 2005.

Quang-Dao Van (Phone: +33 1 41 80 73 80, email: van@univ-paris12.fr), Anne Wei (email: wei@univ-paris12.fr), Benoît Geller (email: geller@univ-paris12.fr), and Gérard Dupeyrat (email: g.dupeyrat@univ-paris12.fr) are with LETIC-IUT de Vitry, the University of Paris XII, France.

by Fig. 1, the additional header consists of a new "IP header," an "ESP header," an "ESP trailer," and an "ESP Auth" [6]. These supplemental fields are comprised between 42 and 56 bytes. Table 1 displays the overhead proportions in a datagram for a typical 1,000-byte video packet size. These overheads degrade the QoS performance of video transmission.

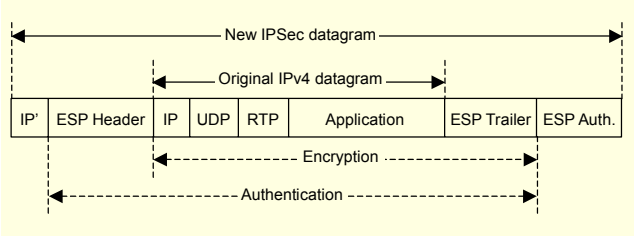

Fig. 1. IPSec datagram in ESP tunnel mode.

Table 1. Additional overhead in size and percentage.

Protocol	Overhead	Size (bytes)	Percentage
IPv4	RTP/UDP/IP	12/8/20	4 %
IPSec	IP´	20	8.2-9.6%
	ESP Header	8	
	RTP/UDP/IP	12/8/20	
	ESP Trailer	2-16	
	ESP Auth.	12	

B. Security Processing Delay

Data encryption/decryption at each security router involves some security processing delays. We consider that the construction and recovery of an IPSec datagram at any security router take the same amount of time. This delay d_{sec} is evaluated with the following assumption.

Assumption 1. *If N traffics arrive at each security router at rate V (Mbps), and if the security router has a processing capacity of rate R (Mbps), the security router processing delay* d_{sec} *for data encryption or decryption is*

$$d_{\sec} = \frac{N \times V}{R} \alpha , \qquad (1)$$

where the security coefficient α *= 1 second.*

III. Analytical Models for Delay and Loss

1. Delay Analysis

Whatever the protocol involved, there are some fixed delays such as d_{code} delay due to the video encoding, d_{trans} due to the time needed to put a packet on the link, and d_{prop} due to the propagation of the signal on the medium. For instance, these delays can be estimated as follows: to be synchronized, the image part must have a delay close to that of the audio part, and d_{code} = 15 ms is a typical delay of an audio code such as G.729 [7]. Putting a large video packet on a high bandwidth link, e.g. a 1,000-byte size on a 10 Mbps link, requires about 0.8 ms. It takes 4 μs/km for a signal to travel on a coaxial cable and 5 μs/km on an optical fiber cable [1]; so, for a distance of about 10,000 km and with 12 transit routers between the source and the destination (we consider 12 as the average number of routers that an ordinal packet takes in a connection within Europe; for more details, see line 2 of Table 2), one approximately finds that d_{trans} = 10 ms and d_{prop} = 50 ms. The amount of *fixed* delays $d_{code} + d_{trans} + d_{prop}$ to be estimated is thus about 90 ms.

The end-to-end delay in the case of the IPv4 protocol can be written as

$$d_{e2e\_IP} = d_{code} + d_{trans} + d_{prop} + d_{queue} , \qquad (2)$$

where d_{queue} is the waiting time in a router queue.

If IPSec is to be used, d_{e2e_IPSec} must also take into account the security processing delay d_{sec}. The total end-to-end delay in this case becomes

$$d_{e2e\_IPSec} = d_{code} + d_{trans} + d_{prop} + d_{queue} + 2d_{\sec} . \qquad (3)$$

The most variable delay element in both cases is the queuing delay d_{queue}. Suppose that there are H transit routers in a path between a source and its destination; if $d_{h(i)}$ designates the delay at the i-th transit router, the total queuing delay d_{queue} is

$$d_{queue} = \sum_{i=1}^{H} d_{h(i)} . \qquad (4)$$

In order to find $d_{h(i)}$, we make the following classical assumptions: transit routers have a queue implementation at their output ports [8] and these queues are scheduled by First-In-First-Out and DropTail mechanisms; transit routers are connected with a link of capacity C and have a queue length K; and the aggregation of N incoming traffics generated at random moments is considered as a Poisson process with arriving rate $\lambda = \sum_{i=1}^{N} \lambda_i$, where λ_i is the incoming rate generated by the i-th traffic. For a transit router of capacity C, the output rate for forwarding packets toward the output link can be considered as $\mu = C/S_{packet}$, where S_{packet} is the size of a packet incoming at the

transit router. This is a typical model of an M/M/1/K queuing system [9]. In this case, the delay $d_{h(i)}$ is determined by

$$d_{h(i)} = \frac{1}{\mu - \lambda} \times \frac{1-(K+1)\rho^K + K\rho^{K+1}}{1-\rho^{K+1}}, \quad (5)$$

where $\rho = \lambda/\mu$ and $0 < \rho < 1$. Note that the same formulas applied to IPSec to calculate d'_{queue} with different λ and μ values.

2. Loss Rate Analysis

If $l_{h(i)}$ designates the loss rate at the i-th transit router, the total loss rate is $l_{total} = \sum_{i=1}^{H} l_{h(i)}$. In an M/M/1/K queuing system [9], the loss rate $l_{h(i)}$ at each router is given by

$$l_{h(i)} = \frac{1-\rho}{1-\rho^{K+1}} \times \rho^K. \quad (6)$$

As for the delay analysis, formulas also apply to calculate l'_{total}, using λ' and μ', respectively, instead of λ and μ.

Finally, we suppose that all transit routers in the path between a source and its destination have the same behavior and processing capacity, implying that λ and μ don't change at transit routers because the traffic number remains constant due to the "tunneling" mechanism. We thus hold the last assumption:

Assumption 2. *Delay and loss rate are identical for all the transit routers.*

With Assumption 2, $d_{h(i)} \approx d_h$ and $l_{h(i)} \approx l_h$ are identical for any integer i, and the queuing delay d_{queue} and total loss rate l_{total} become

$$d_{queue} = H \times d_h \quad (7)$$

and

$$l_{total} = H \times l_h. \quad (8)$$

3. Estimation of the Number of Transit Routers

We estimated the number of transit routers H between the Web server of the Université Paris XII[1)] source and 50 server destinations around the world. The results are gathered in Table 2. We chose H=12, the average number in continental communication, which will be used in the results displayed in section IV.

1) Trace collected by Traceroute tool. Server destinations consulted at http://www.traceroute.org

Table 2. Average number of transit routers from the Université Paris XII to various destinations.

Server location	H
France metropolitan	7-14
Western Europe	9-15
U.S.A.	13-21
Eastern Asia	17-25

IV. QoS Estimation

1. Video Generation

We consider a constant bit rate (CBR) video, encoded in the coding standard H.261 [10]. Video packets at the application layer are encapsulated at the transport layer by the real-time transport protocol (RTP) and user datagram protocol (UDP) pair before being passed to the network layer.

The parameters used in our numerical calculations are gathered in Table 3.

Table 3. Parameter settings.

Param.	Value	Param.	Value
V	64, 384, 1536 kbps	R	80 Mbps
K	30-300	C	10 Mbps
S_{video}	1000 bytes	H	4-12

2. QoS Requirements

A. End-To-End Delay

In order to provide quality and interactivity of video, the end-to-end delay must be minimized. The ITU-T Recommendation G. 114 [1] recommends keeping the one-way delay under 150 ms.

B. Loss Rate

As for any real-time traffic, a lost video packet is not re-transmitted. Loss reduces the quality of the perceived video and must be minimized. This paper proposes that the total loss rate l_{total}, defined as the total number of packets lost over the total number of packets sent, must not exceed 1%.

3. Results

We display several end-to-end delays d_{e2e} in the case of three classes of bit rates: V = 64, 384 and 1,536 kbps. These bit rates correspond respectively to low, medium, and high quality

video conferences [11]. Figure 2 displays the end-to-end delays obtained for both IPv4 and IPSec protocols.

One can see that contrarily to the IPv4 case, the end-to-end delay in the IPSec case grows rapidly with the total traffic; this is due to the security processing delay for encryption/decryption and to the additional overhead. In other words, this shows that the number of video traffics is reduced by a factor from 4 for high quality video to 6 for low quality video. One can notice that the IPSec protocol limits the number of high quality video traffics to be transmitted.

Figure 3 displays the total loss simulated with the same scenarios. Contrarily to the important degradation observed with the end-to-end delay, losses are only slightly worse with IPSec compared to IPv4. The loss rate is not a critical parameter because the tolerated loss target is 1%. This is due to the "tunneling" mechanism, which keeps the same video traffic number at any transit router. This holds true when we consider variable queue lengths (K from 30 to 300).

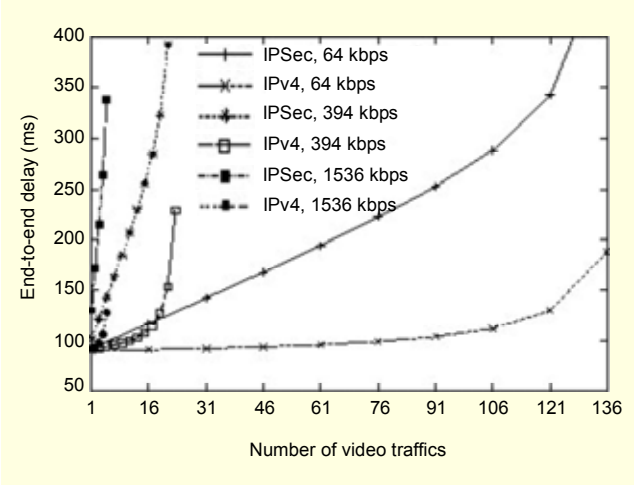

Fig. 2. End-to-end delay vs. number of traffics.

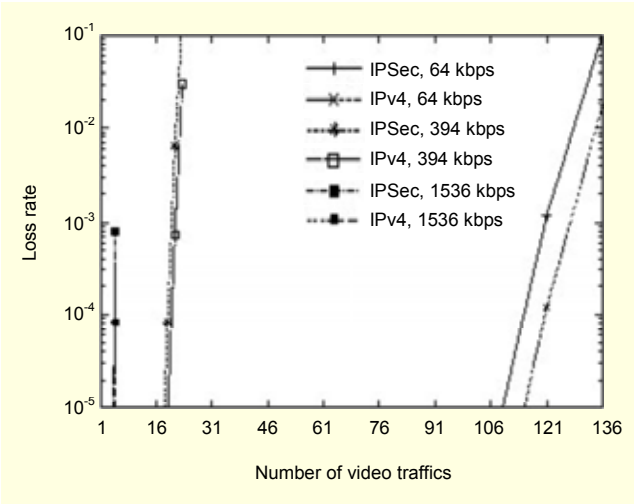

Fig. 3. Total loss rate vs. number of traffics.

V. Conclusion

IPSec is one of the promising solutions for securing the video traffics over an IP network. In this paper, we compared the QoS of CBR video traffics over an IP network when IPSec and the original IPv4 are applied. On one hand, the analytical results clearly show that the security processing with IPSec increases significantly the end-to-end delay; the effect is even more significant for low quality video. On the other hand, the packet loss rate is not really affected when IPSec is applied. A more complete work could estimate the performance with other parameters than the parameters gathered in Table 3. Also, in order to support both QoS and security with IPSec, a future work will consider adding some QoS parameters into the IPSec Security Associations.

References

[1] ITU-T Std. G.114, *General Characteristics of International Telephone Connections and International Telephone Circuits: One-way transmission time,* 1996.

[2] Cisco System Inc., *Cisco VPN Security Router,* 2002. http://www.cisco.com/en/US/products/hw/routers

[3] R. Barbieri, D. Bruschi, and E. Rosti, "Voice over IPSec: Analysis and Solutions," *Proc. IEEE Annual Computer Security Applications Conference,* Jun. 1996, pp. 261-270.

[4] S. Ariga, M. Minami, H. Esaki, et al., "Performance Evaluation of Data Transmission Using IPSec over IPv6 Networks," *Proc. INET2000*, Jul. 1996.

[5] IETF Std. RFC 2401, *Security Architecture for Internet Protocol,* Nov. 1998.

[6] IETF Std. RFC 2406, *IP Encapsulating Security Payload ESP,* Nov. 1998.

[7] P. Collet, M. Dudent, and O. Hersent, *Téléphonie sur l'Internet : quelles perspectives,* FT R & D, 1998.

[8] F.A. Tobagi et al., "Service Differentiation in the Internet to Support Multimedia Traffic," *Proc. IWDC,* Sept. 2001.

[9] T.G. Robertazzi, *Computer Networks and System: Queuing Theory and Performance Evaluation,* Springer, 2000.

[10] ITU-T Std. H.261, *Video Codec for Audiovisual Services at p*64 Kb/s,* 1993.

[11] I. Dalgic and F.A. Tobagi, "Constant Quality Video Encoding," *Proc. IEEE ICC*, Jun. 1995, pp. 1255-1261.