Secure Transmission for Interactive Three-Dimensional Visualization System

pISSN 2383-5389 / eISSN 2383-8116

Journal of International Society for Simulation Surgery 2017;4(1):17-20 https://doi.org/10.18204/JISSiS.2017.4.1.017

ORCID
H.Y. Yun:
Sun Kook Yoo: orcid.org/0000-0002-6032-4686

Secure Transmission for Interactive Three-Dimensional Visualization System

H.Y. Yun, Sun Kook Yoo

Medical Engineering, Yonsei University College of Medicine, Seoul, Korea

Purpose Interactive 3D visualization system through remote data transmission over heterogeneous network is growing due to the improvement of internet based real time streaming technology.
Materials and Methods The current internet's IP layer has several weaknesses against IP spoofing or IP sniffing type of network attacks since it was developed for reliable packet exchange. In order to compensate the security issues with normal IP layer, we designed a remote medical visualization system, based on Virtual Private Network.
Results Particularly in hospital, if there are many surgeons that need to receive the streaming information, too much load on the gateway can results in deficit of processing power and cause the delay.
Conclusion End to end security through the network method would be required.

Key Words Secure · Transmission · Interactive · Visualization · Three dimension.

Received: May 17, 2017 / **Revised:** May 19, 2017 / **Accepted:** May 22, 2017

Address for correspondence: Sun Kook Yoo
Medical Engineering, Yonsei University, 50-1 Yonsei-ro, Seodaemun-gu, Seoul 03722, Korea
Tel: 82-2-2228-1919, **Fax:** 82-2-363-9923, **E-mail:** sunkyoo@yuhs.ac

Introduction

Interactive 3D visualization system through remote data transmission over network is growing due to the improvement of internet based real time streaming technology. Since the transmitted image data with DICOM (Digital Imaging and Communications in medicine) format contains important medical parameters such as the patient's health record and image data, omission, or alteration of the transmitted data is crucial. However, the current internet's IP layer has several weaknesses against IP spoofing or IP sniffing type of network attacks since it was developed for reliable packet exchange. Therefore, it is unsafe and unreliable to use the commercial network to transmit important medical information.

In order to compensate the security issues with normal IP layer, the protocol named Virtual Private Network, VPN, has been developed. VPN offers enhanced security feature using a tunneling protocol over the public network that passes through the private network's traffic to protect IP packet in network layer, and assures integrity and data-origin authenti-cation using IPsec.

This research emphasizes the possibilities of implementing security in real time medical diagnosis over the commercial network by measuring the effect on the network between nodes while using AH and ESP protocol which are compatible with IP layers, and moreover, to use the results as a reference when developing telemedicine system policy.

Materials and Methods

Secure Network Protocol Analysis

Public network operates over VPN (Virtual Private Network) to secure data transmission. A protocol called VPN pro-tocol is used to form a tunnel and it is categorized by where it is operated and based on 2nd, 3rd or 5th layer tunneling pro-tocol in OSI (Open Systems Interconnection) reference model. Especially, 3rd layer tunneling protocol uses a packet and IPSec is one of the common 3rd layer tunneling protocols that is IETF standard. IPSec encrypts IP packet by adding an extra header before it sends the packet over the network. IPSec consists of three protocols called SA (Security Associa-tion), AH (Authentication Header), and ESP (Encapsulation Security Payload).

In order to transfer data safely, agreements about password algorithm, key exchange method, and key exchange be-tween sender and receiver have to be established before communicating an authorized or encrypted data. The components that need to be agreed before exchanging data are called SA (Security Association) in IPSec. AH offers security services such as access control, connectionless integrity, and data-origin authentication, and preferably choose to set up an anti-reply service. The integrity is calculated at every 512bit block, and MD5 (Message Digest) which processes the 128-bit hash and SHA-1 (Secured Hash Algorithm) which processes 160-bit hash are guaranteed by the message authentication code of message compression algorithm, and the authentication is guaranteed by the public key (1).

ESP offers encryption of packet, integrity, and replay. ESP can also offer an authorization services, nevertheless, it cannot perform IP header authorization which AH can offer. Moreover, ESP protocol offers data privacy that includes all the functions in AH to protect attacks from encrypted but unauthorized data streams. ESP uses shared symmetric key to encrypt and decrypt DES function every 64bit block (2).

Depending on where the protocol header is located, AH and ESP protocol operated in either transport mode or tunnel mode. Transport mode puts the security header between packet header and payload in IP packet and therefore it protect upper level protocol data such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Encryption method in VPN can be categorized into three types; between hosts, between host and security gateway, and between security gateways. A gateway system mediates distrusted external system and trusted internal subnet system, and it offers security service to the trusted internal host. When a security gateway provides a service in a replacement for more than one subnet host, the gateway creates SA for the hosts and offers security service between the security gateway and an external system. In this case, only the gateway requires to embody AH (Authentication Header) and ESP (Encapsulating Security Payload), and all the systems that use the gateway in the trusted subnet can use AH and ESP service through the gateway. In reality, since the IPSec is processed between security gateways, there is no load in the host nor required to setup the host. However, if there are too many terminals that require tunneling, a delay could occur due to the increased load in the gateway. If one of them is a gateway instead of a host in security communication, one must apply the tunneling mode. The tunneling mode could be applied between hosts as well.

Theoretically, when transmitting in the transport mode, there is 24bytes and 22bytes increase in size of data for AH and ESP, respectively, since the security header information is added to each packet. In contrast, there is 44bytes and 42bytes increase in size of data for AH and ESP, respectively, since new header information is also added in addition to the security header.

System Requirement

For real-time transmission of medical images for interactive operation, the following patient' information is required; radio-

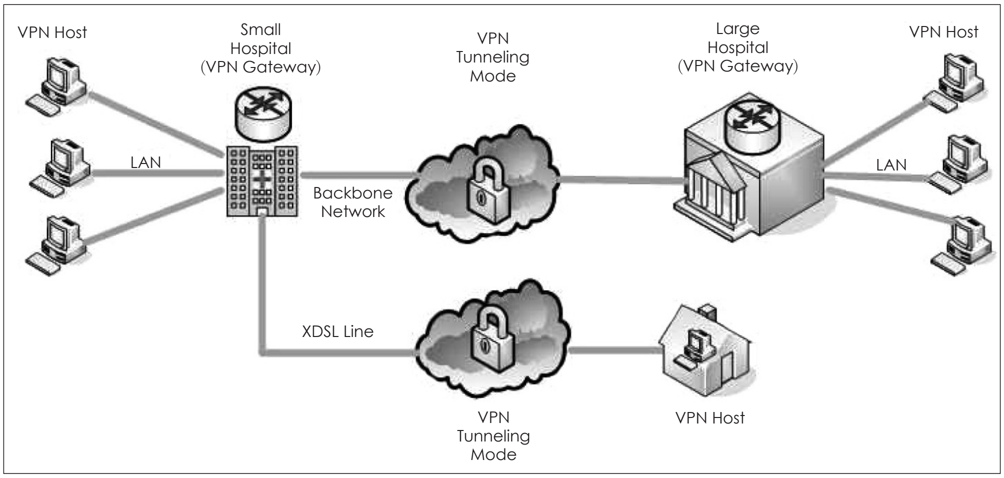

Fig. 1. Network Test.

logical data such as X-ray, CT, and MRI images

As well as medical record data that contains the patient's chart information (Fig. 1).

Before to start the real test where a small hospital and a general hospital is connected, we applied the algorithm to the LAN under the Host-to-Host Mode in pretest. We assumed Host 1 as a doctor and Host 2 as a patient, then transmitted the patient image with medical record data packet from Host 2 to Host 1 under the transmission mode.

From a small or medium sized hospital, the real-time streaming of a patient's status is sent using the backbone network to either a general hospital or the duty surgeon's home for review. Each hospital is connected through the backbone network and the duty surgeon's home is connected through home network. If a gateway is present, for example, a general hospital, only with IPSec between gateway-terminals can maintain security in the private network.

Results

Real-time data maintains relatively steady data throughput compare to the dummy data transmission. In 100Mbps test setup, the dummy data transmission uses the maximum bandwidth, but the telemedicine data maintains the maximum of 2Mbps throughput since it is time-dependent. Throughput decrease in IPSec setup assures the minimum of 80%.

The total transmission time that takes to reach the terminal upper application layer in IPSec setup is shown above. In IPSec, the calculation time is proportional to the increase in number of DES block processes. ESP delay increase in is more than AH delay increase since MD5 algorithm in AH is processed every 512bit and DES algorithm in ESP is pro-cessed every 64bit.

The overhead was large when both AH and ESP was used for more powerful authorization than ESP was used alone (increased up to 9%). This is because there is a delay in encrypting and decrypting the newly added header. IPSec showed the lowest performance at Windows stage. This reflects the lowest data transfer efficiency due to increased packet data amount, process time, and transmission hop.

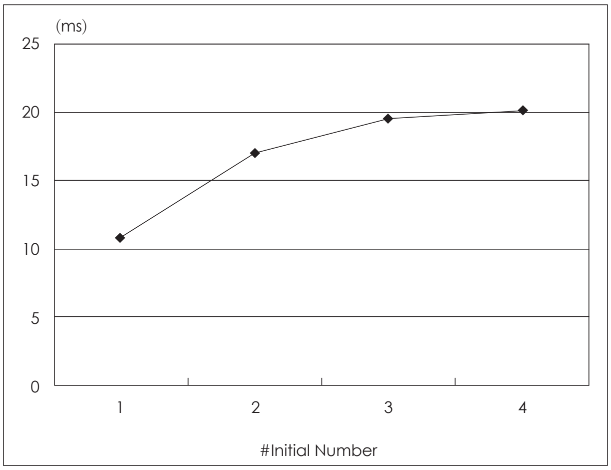

Fig. 2. Total transmission time when IPSec is applied to hosts in the private network.

When we compare the transmission time with or without security feature, a big jitter value appeared in IPSec security process (increased up to 364%) (Fig. 2). This shows that it might influence the real time streaming when there is interference in the encrypting and decrypting unit due to extra processing. Jitter value increased when bigger size data was secured as the number of block processes increase when we compare each jitter value. Also, there was more delay in processing AH in Windows stage than Linux stage because AH is applied to all the nodes not only between gateways when security feature is applied to the gateway and therefore overall size of the data is increased.

When AH and ESP were applied to the gateway, delay in transmission time due to increased in number of hosts is in-creasing. As number of hosts increase, delay increases exponentially because there is not enough processing power as encapsulation and decapsulization processes increase.

When the specialist is out of the hospital or at home, the test result between hosts in the private network is as follows. The basic transmission time showed more than 10 times of delay due to the available bandwidth and interference with other users. Nevertheless, it is below the ITU restricted the maximum delay of 150ms and therefore applicable to the interactive three-dimensional visualization system.

Discussion and Conclusions

We could see from the pretest that the security of IP and Packet would be guaranteed only if AH and ESP are used to-gether. In other word, we have to use AH and ESP at the same time to resolve the important security problems occurring during the transmission of the medical information in real time.

In testing environment, it was found that the delay caused by encryption and decryption was greater than the delay due to increased in size of data in real-time streaming of medical information securely. An increase in size of transmitted data was the maximum of 12% respect to non-IPSec packet. This means it is required to keep the bandwidth below 86.3% of the real bandwidth of the private network in order to prevent the overload caused by increased IPSec data. When IPSec is applied, it might be unstable to stream the real-time data because the delay is sufficient. Similar to the scenario, such as in a general hospital, if there are many surgeons that need to receive the streaming information, too much load on the gateway can results in deficit of processing power and cause the delay when using IP-Sec, as well. Hence, end to end security through the network method would be appropriate if there are many professional surgeons that need to receive the real-time streaming of medical information.

Moreover, due to the characteristics of wireless environment, the security between wireless access point and terminals is important. Nevertheless the secured transmission would be delayed at surgeon's level due to the decryption processing delay caused by low performance of portable or tablet PC (Personal Computer) compare to wired PC.

Interactive 3D visualization system through remote data transmission over network is growing due to the improvement of internet based real time streaming technology. However, the current internet's IP layer has several weaknesses against IP spoofing or IP sniffing type of network attacks since it was developed for reliable packet exchange. In order to compensate the security issues with normal IP layer, we designed a remote medical visualization system, based on Virtual Private Network.

References

1. Microsoft Corporation, "Web Workshop-Virtual Private Networking: An Overview," http://msdn.microsoft.com/workshop/server/feature/vpnovw.asp, May 1998
2. www.cs.ucsd.edu/users/bsy/dobbertin.ps
3. Peter B. Angood. Telemedicine, the Internet, and World Wide Web: Overview, Current Status, and Relevance to Surgeons. World Journal of Surgery 2001;25;1149-1457
4. Chen, T.M. Network Traffic Measurement and Experiments. IEEE Communications Magazine 2000:120-185
5. Victoria Fineberg, A Practical Architecture for Implementing End-to-End QoS in an IP Network, IEEE Communication Magazine, January 2002
6. IBM, "VPN Overview," IBM Networking White Papers: Voice-Data Integration in ebusiness, http://www.networking.ibm.com/vpn/vpntech.html.
7. John P. McGregor and Ruby B.Lee, Performance Impact of Data Compression on Virtual Private Network Transactions. IEEE Communication Magazine 2000;500-510