The Effect of Security on Performance in a VoIP Network using An Analytical Simulator

Ohnmar Nhway
University of Computer Studies, Mandalay
skynhway@gmail.com

Abstract

Nowadays, Voice over IP (VoIP) is a major and challenging task for communication technology. In this paper, we focus on VoIP which transmits voice over packet switched networks such as LANs or WANs. Adding security to a VoIP system, the quality of service and performance of the system are at risk. The contribution of this paper has two main parts; firstly it illustrates registration call setup using Diffie-Hellman Key Exchange Algorithm. Secondly, it evaluates two key performance of a VoIP: delay and bandwidth using an analytical simulator. The processing steps of this paper are: the Key Exchange Algorithm generates a key to provide authentication. The generated key is used by AES Algorithm to secure the signaling and voice traffic within a VoIP system based on SIP (Session Initiation Protocol) server. In addition, Counting Process in Stochastic Processes is also used for call breakdown.

Keywords: RTP, Security, Simulation, SIP, Network Design, VoIP.

1. Introduction

Voice conversations applied VoIP technology for transmission using the IP (Internet Protocol) over a network with packets of data. The data network such as the Intranet or more likely the Internet has changed the strategy adopted by telecommunication managers. It is, therefore, one of the highest growth areas.

VoIP calls can take place between LANs or on WANs, as is the case with internal calls on a corporate network. If a VoIP user wishes to call a destination on POTS, a special gateway is used. These devices translate the incoming data into a format the recipient, be it IP, can understand.

In VoIP system, the aim of the conversion is to reduce the costs to home and business users by standardization of the network infrastructure. The popularity of VoIP is increasing rapidly due to cheap calls worldwide.

On the other hand data networks utilize packet switching and so a dedicated circuit does not exist, a virtual circuit is created, making the network much more efficient. Voice information is sampled and converted to digital form before being assembled into packets which are transmitted over the IP network. Each data packet contains the source and destination IP address and is routed to the destination using the level 3 routing mechanism prescribed in the network. At the destination these packets are then disassembled and played to the user as seen in Figure 1[1].

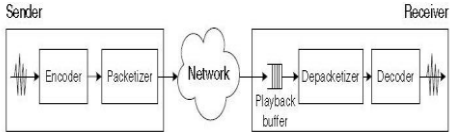


Figure 1. Components of a VoIP system

VoIP and related real-time communication applications, such as video conferencing and instant messaging, continue to attract considerable interest worldwide, with millions of active private business VoIP users today [2].

This paper emphasized the security effect of performance in VoIP scheme, which is based upon ad-hoc network through the voice and Diffie-Hellman Key Exchange Algorithm in cryptosystem for using registration. On the other hand, registration means to check user identify correctly. Moreover, an analytical simulator utilizes techniques used for network flows and queuing network analysis to compute two key performance bounds for VoIP: delay and bandwidth.

The rest of this paper is organized as follows. Section-2 introduces the properties of VoIP Network. Section-3 presents the proposed methodology of VoIP security process how to apply the requirement materials. Section-4 describes experimental study using an analytical simulator in detail. Finally, Section-5 concludes the study and identifies the future research.

2. Properties of VoIP Network

There are several steps in the process of transmitting voice sounds over a channel: sampling, digitizing, encoding, transport, decoding, and playback in a VoIP Network. The main factors that affect standards, the quality of services and VoIP codec characteristics are shown in Table 1[3], 2 [3]and 3[4].

Table 1. ISO Reference Model and VoIP Standards

ISO Protocol layer	Protocols and standards
Presentation	Codecs/Applications
Session	H.323/SIP/MGCP
Transport	RTP/TCP/UDP
Network	IP
Link	FR, ATM, Ethernet, PPP, etc.

Table 2. Recommendations of International Telecommunication Union

Delay	For high quality voice, one way latency must not be greater than 150ms. Delay greater than 50ms leads to echo and talker overlaps.
Jitter	Variation in inter-packet arrival time. The solution to this problem is to introduce jitter buffers.
Packet Loss	Loss in excess of 5-10% causes significant degradation in voice quality.
Re-ordering	Packets may arrive out of order and this leads to garbled speech.
Speech Coding	PCM

Table 3. VoIP codec characteristics

Codec	Algorithm	Bandwidth used for sound	Packet interval	Voice bits per packet	Processing intensity
G.711	PCM	64 kbps	20 ms	1,280 bits	Low
G.726	ADPCM	32 kbps	20 ms	640 bits	Medium
G.728	CELP	16 kbps	10 ms	160 bits	High
GSM	CELP	13 kbps	20 ms	160 bits	Depends upon algorithm used; CELP is higher

3. Proposed Methodology of VoIP Security Process

Communication is one of most important roles for all over the world to connect each other. For example, VoIP systems (Skype, Gtalk and so on) used together with user name and password account. In this fact, this paper used Key Exchange Algorithm instead of user and password account for security between two parties. On the other side, the paper created registration using Key Exchange Algorithm such as authorized users. In this way, this paper presented to secure the voice data between caller and callee using AES encryption/ decryption

processes based on Diffie-Hellman Key Exchange Algorithm [5].

In this system, VoIP scheme is made up of four phase approaches;

(i) registration,

(ii) call setup,

(iii) transmission of the voice information and

(iv) breakdown of the call.

3.1. VoIP Registration and Call Setup

If user wants to speak another person, this user must register as an authorized user for using registration function. Here, registration utilizes Diffie-Hellman Key Exchange Algorithm in Table 4.

Table 4. Diffie-Hellman Key Exchange Algorithm

Global parameters	
q	prime number
α	$\alpha < q$ and α is a primitive root of q
Caller's Key Generation	
Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = (\alpha)^{X_A} \bmod q$
Callee's Key Generation	
Select private X_B	$X_B < q$
Calculate public Y_B	$Y_B = (\alpha)^{X_B} \bmod q$
Calculation of Secret Key	
$K = (Y_B)^{X_A} \bmod q = D_i$,	$K = (Y_A)^{X_B} \bmod q = V_i$

In the following equation, assumes such as Caller means D_i and Callee also means V_i [6][7].

$$R(x) = D_i - V_i \begin{cases} \text{Accept, } R(x) = 0 \\ \text{Reject , otherwise} \end{cases}$$

where, R(x) = registration function

D_i = caller's secret key

V_i = callee's secret key

3.2. Central Directory

If the central directory is trusted, then this form of communication provides both confidentiality and a degree of authentication. Because only Caller and Callee can determine the key, no other user can read the message (confidentiality). Recipient Callee knows that only Caller could have created a message using the generated key (authentication) [7].

3.3. Transmission of Voice Information

Encryption is one of the essential security technologies for computer data, and it will go a long way toward securing VoIP. Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

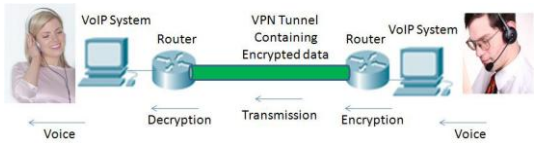


Figure 2. The use of VPN with IPSec

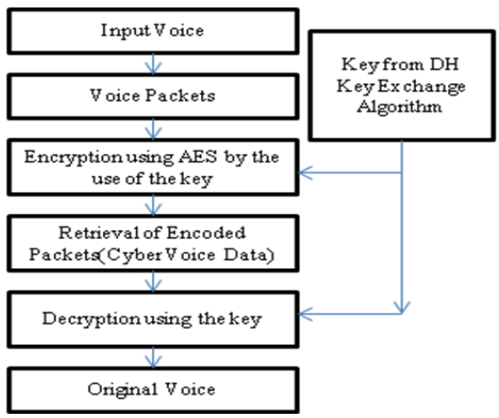


Figure 3. Encrypt and Decrypt using Key from Diffie-Hellman Key Exchange Algorithm

Similarly the Figure 2 and 3 will help to encrypt and decrypt data using key from the Diffie-Hellman Key Exchange Algorithm based on a Virtual Private Network (VPN). The input voice is digitized and encrypted based on AES using key which is generated from the Key

Exchange Algorithm. The same encrypted data also decrypted from the receiving end based on AES using the generated key.

An encryption algorithm along with a key is used in the encryption and decryption of data. AES is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. It has been analyzed extensively and is now used widely world wide enough protect classified information up to the top secret level. AES supports key sizes of 128 bits, 192 bits and 256 bits and will serve as replacement for the Data Encryption Standard which has a key size of 56 bits.

This paper utilizes AES (Advanced Encryption Standard) Algorithm for encrypting and decrypting of voice data.

A triplet (Gen, Enc, Dec) of algorithms, a message space M and a key space K, is called a symmetric key encryption scheme if:

(a) The key-generation algorithm:

Gen is an algorithm that returns a key K using Diffie-Hellman Key Exchange Algorithm, denoted by k ←□ Gen, such that k∈K.

(b) The encryption algorithm:

Enc is an algorithm that takes a key k and a voice data m ∈□ M, and outputs a cipher data c□← Enck(m).

(c) The decryption algorithm:

Dec is an algorithm that takes a key k and cipher data c and outputs a voice data m.

The scheme should satisfy the following property: For all m ∈M and k ∈K,

$$[\ Dec[k]\ (\ Enc[k]\ (\ m\ )\ )\ =\ m\ ]$$

Where, Enc = Encryption Algorithm,
Dec = Decryption Algorithm

This paper is discussing about the key generation method using Diffie-Hellman Key Exchange Algorithm in Cryptosystems [5].

3.4. Breakdown of the call

In the counting model, we find out two facts. The limitation call's times subtract the number of call's times. If the result is greater than or equal to the zero, there is no error. Then both sender and receiver continue to communicate and start conversation each other. So, we solve for this case using Counting Process in Stochastic processes.

For example, the event limits for making between "0" to "t" times. This event processes during starting "0" time to finishing "t" times ((0, t]) [8].

$$G(x) = t \quad - \sum_{i=1}^{n} i \begin{cases} \text{accept, } 0 \le g(x) \\ \square \le t \end{cases}$$

where,

G(x) =counting function of ultimate destination
t = limitation time
n = number of call time, events

4. Experimental Study

The experimental setup was carried out over a LAN environment. The two end systems were interconnected over 100 Mbps. The application of voice transmission is based on rtptools and robust audio tool. This system uses PCM(64 Kbps) data for primary data whose sampling rate is 8000 Hz for redundant data as experiment data [9].

The simulator also has an engine that automates and implements the analytical techniques. The engine determines the number of VoIP calls that can be sustained by the constructed network while satisfying VoIP QoS requirements and leaving adequate capacity for future growth.

As an experimental study, the paper illustrates how the simulator can be utilized to assess the readiness to deploy VoIP for a typical network of a small enterprise [10].

Table 5 describes the "Properties" which is used to specify the properties of the network elements of nodes, links and subnets (such as name, bandwidth or capacity, location, width, height and the background traffic).

Table 5. Properties of the network elements of nodes

F1C1	< ------ >	F1SW
F1SW	< ------ >	Switch 1
Switch 1	< ------ >	Router
Router	< ------ >	Switch 2
Switch 2	< ------ >	VoIP Gateway
F1C1	< ------ >	F1C2
F1C1	< ------ >	VoIP Gateway
F2C1	< ------ >	F2C2
F2C1	< ------ >	F3C2
F2C1	< ------ >	VoIP Gateway
F3C1	< ------ >	F3C2
F1C1	< ------ >	F3C2
F1C1	< ------ >	F2C2
F3C1	< ------ >	VoIP Gateway

Figure 4 illustrates corresponding network infrastructure constructed by analytical simulator in detail.

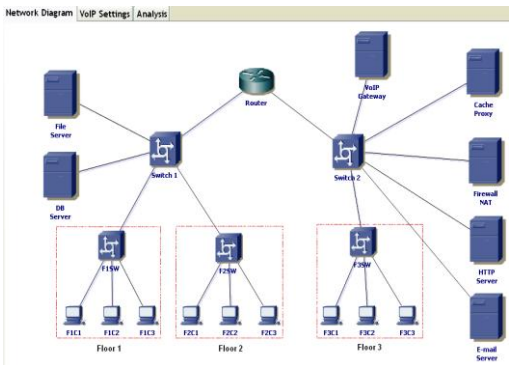
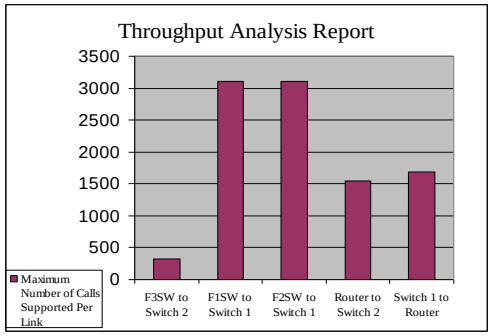
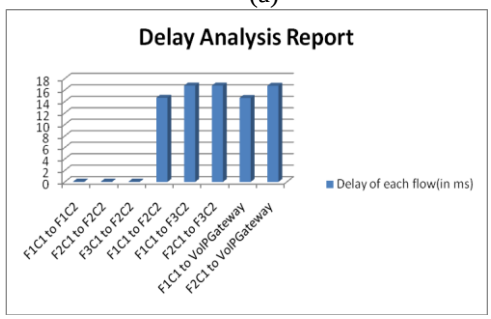


Figure 4. Corresponding network diagram constructed by analytical simulator



(a)



(b)

Figure 5. Throughput Analysis Report(a) and Delay Analysis Report(b)

Figure 5(a) and (b) shows the reports of throughput and delay analyses. Moreover, Figure 5(a) reports the number of calls that can be supported based on bandwidth analysis. As a result of the router is the bottleneck, and supporting calls more than 315 calls would require definitely a replacement for the router. Figure 5(b) shows that with 313 calls and a network delay of 16.76 ms during F1C1 to F3C2 and F2C1 to F3C2. This means when adding one more call, the network delay of a maximum of 80 ms was exceeded. The report of Figure 5(b) also exhibits the network delay per flow or path.

This experimental result, there were a total of nine VoIP flows. As shown, the first triple is for intra-floor flows. The second triple is for inter-floor flows. And the third triple is for external flows.

So, the network delay (for this particular network topology) is the more dominant factor (than throughput) in determining the number of voice calls to be supported for real world network using this simulator.

5. Conclusion and Future Research

The paper is developed to provide security for voice data and how to prepare the network infrastructure for VoIP. Generally passwords and smart cards are used for the security systems. The paper enables to generate a key from Diffie-Hellman Key Exchange Algorithm for the security system of VoIP Network. The generated key is used by AES Algorithm for encryption/ decryption process to secure the signaling and voice traffic within a VoIP Network. In addition, the paper also emphasizes Counting Process in Stochastic Processes. Moreover, the paper evaluates the performance of a VoIP system for delay and bandwidth using an analytical simulator.

Later, the paper will be analyzed registration, call setup, voice transmission packets with novel method of Biometric Fingerprint. The Biometric Fingerprint also produces a key that is used by AES Algorithm to secure the signaling and voice traffic within a VoIP system in my future research.

Acknowledgements

First and fore most, I wish to express my deepest gratitude to my parents and my relations for their encouragement, understanding and support throughout the period of doing my Ph-D candidate.

Finally, my special thanks are due to all my teachers who taught me and gave their knowledge to me from kindergartens (primary school, high school, UCSY) to UCSM.

References

[1] Syed A. Ahson, Mohammad Ilyas, *VoIP HANDBOOK: Applications, Technologies, Reliability, and Security*, CRC Press, Boca Raton London, New York, 2009, pp. 3-23.

[2] J. Skoglund, E.Kozica, J.Linden, R.Hagen, W. B. Kleijn, "Voice over IP ; Speech Transmission over Packet Networks", Springer Handbook of Speech Processing, Benesty, Sandhi, Huang, 2008, pp. 308, 309, 310, 311,313, 314.

[3] VoIP powerpoints from http://www.wikipedia, Cisco, 2010.

[4] Theodore Wallingford, *Switching to VoIP*, June 2005, pp.44.

[5] Ohnmar Nhway, "An Investigation into the Effect of Security on Reliability and Voice Recognition System in a VoIP Network", IEEE The 13th International Conference on Advanced Communication Technology, Republic of Korea, Feb 13~16, 2011, pp.1293~1297.

[6] May Phyo Oo, *Managing Certificates of Grid Security Infrastructure*, Ph.D(IT), University of Computer Studies, Yangon, Myanmar, 2007.

[7] William Stallings, *Cryptography and Network Security Principle and Practices*, Fourth Edition, pp. 298, 484, 492.

[8] Sheldon M. Ross, *Stochastic Processes*, University of California, Berkeley, 1983.

[9] Thinn Naing, Moe Pwint, "FEC-based Loss Control Mechanism for Optimizing Voice Communication Quality", Proceedings of the seventh International Conference on Computer Applications, Yangon, Myanmar, 2009, pp.129.