IJCSC International Journal of Computer Science & Communication Vol. 1, No. 2, July-December 2010, pp. 101-104

Effective Realization of QoS, Network Scalability in Term of Network Security using Symmetric Algorithm

Sharad Patil[1] & Ajay Kumar[2]

[1]Research Student, Bharti Vidyapeeth, Pune, India
[2]Jaywant Management Institute, Pune(MS), India
Email: [1]sd_patil057@rediffmail.com, [2]ajay19_61@rediffmail.com

ABSTRACT

Computer networks able to support multimedia applications with diverse QoS performance requirements are evolving. To ensure that multimedia applications will be guaranteed the required QoS, Presently, there are various kinds of networks; wired and wireless that co-exists with each other. These networks have QoS characteristics that are drastically different and whose degree of variability of the different QoS parameters, such as bandwidth, delay and jitter, differ considerably. There are different network design properties may result in congestion even with network of unlimited bandwidth. Here we consider different security [encryption/ authentication] algorithm and it's evaluation performance for diff. Packet size and throughput for ESP and QoS. The goal of this paper is to put all of this into perspective and provide holostic view of the need for and the value of creating a QoS enabled network.

Keywords: ESP, IPSec, QoS, Security, Protocols

1. INTRODUCTION

QoS is the ability of the network to provide a service at an assured service level while optimizing the global usage of network resources. IPSec is a protocol that allows to make secure connection between branch offices and allows secure VPN access. IPSec is designed to provide inter-operable cryptographically –based security for Ipv4 and Ipv6. IPSec operates at the layer, making it transparent to applications and users. In general, protection mechanism require more processing time and cause traffic delay, real-time application such as video conferencing, VoIP, and real-time video need special processing to achieve their goals and to overcome the delay introduced by adding security mechanism. QoS has been emerged to solve a pert of this problem by providing priority treatment to real time traffic. In the Quality of Service [QoS] domain, the class of service concept divides the network traffic into different classes and provides a class-dependent service to each packet.to classify the each packet is assigned a priority value.

We use the term *Quality of Security Service* to refer to the use of *security* as a quality of service dimension. To recap, the enabling technology for both QoSS and a security-adaptable infrastructure is *variant security*, or the ability of security mechanisms and services to allow the amount, kind or degree of security to vary, within predefined ranges. This notion of network Quality of Security Service has the potential to provide administrators and users with more flexibility and potentially better service, without compromise of network and system security policies.

The protocols used for negotiating QoS agreements may be subject to attack or interference by non-participating parties.

Security services such as encryption can prevent delay requirements from being met by introducing additional latencies. Algorithms whose timing is data dependent may introduce additional jitter, as well. Irregular operations such as re-keying may do this also.

Security services can benefit from QoS measures, as well. To the extent that QOS measures limit delay and jitter, control of such features as a covert signaling measure is depreciated.

To the extent that QoS operates under a business model that requires assurance of network management services for provisioning, auditing, and billing, the QoS mechanisms may well take advantage of existing network security services. Both QoS and security are resource management problems and conflicting demands for limited resources are to be expected.

This paper divide in different section for more elaboration as follows section-II, Section-III, Section-IV, V etc.

2. QOS ELEMENTS

We can divide Quality of Service into the following three layers:

Application Level Quality of Service: Specifies those parameters related to user requirements and

This document was created using SOLIDPDFTools To remove this message, purchase the product at www.SolidDocuments.com

expectations. Frame size, sample rate, image and audio clarity are some parameters of this level.

System Level Quality of Service: Includes operating system and CPU requirements, such as processing time, CPU utilization, and media relations like synchronization.

Network Level Quality of Service: Defines communication requirements, such as throughput, delay, jitter, loss, and reliability.

To realize and implement QoS parameters in a network, the following characteristics of network traffic need to be explained: packet classification, congestion management, congestion avoidance, traffic-shaping and policing and Link efficiency management.

QoS provides better qualities for any particular traffic eg. Voice or IP, video conferencing and text basis. We also use for security purpose for stopping threat Vulnerabilities, use some formula whenever link will be low for any QoS base application.

3. METHODOLOGY

Our Basic intension How QoS provide security features, Such as applying policies and QoS trusting and scheduling the effects of unwarranted traffic or malicious attacks. For eg. Trusting and scheduling important data network traffic over unmarked data traffic might yield additional stability in the event of a denial of service [DOS] attack. Through policing, QoS limits an attackers ability to impose or steal information, Although QoS cannot prevent theft of information. It can limit this behavior by explicitly discarding or limiting associated traffic.

Here we are using two routers –7200 series, Ram-256,Ios as a basic device for testbed and QoS Device manager software as tools. Consider the concept of ESP Encapsulating Secuirty Payload [ESP] provides the framework for the data confidentiality, data integrity, data origin authentication and optional anti-reply features of Ipsec. While ESP is the only IPSec protocol that provides data encryption. It also can provide all of the Ipsec features, because of this, ESP is primarily used in Ipsec VPNs today. The following encryption methods are availableto IPSec ESP.

Data Encryption Standard [DES]- an older method of encrypting information that has enjoyed widespread use. AES[Advanced Encryption Standard[AES] – One of the most popular symmetric key algorithm used today. Triple Data Encryption standard [3DES] – A Block cipher that uses DES three times.

In this Paper we consider 3-DES symmetrical secuirty algorithm, can be used to encrypt large amount of data. IPSec authentication provides through MD-5 with http traffic, downloading 6 mb text file. The follwing test consider the parameter like BW testing – 1.5 mbps, delay 33 mS, and apply the load 1024 bytes, reliability 1 and clock rate- 1500000 and each packet observed 3 minutes max. here providing diff. Packet size and observe the bandwidth without QoS and applying QoS as below.

4. QOS AND SECURITY

There are five parameter must be coordinated during quick mode between Ipsec peer.

- IPSec protocols [ESP or AH].
- IPSec encryption types[DES, 3 DES,AES].
- IPSec authentication[MD5 / SHA-1].
- IPSec mode [tunnel or transport].
- IPSec SA lifetime [Seconds or kilobytes].

Qualtity of Service is board term used to describe overall experience a user or application will receive over network. QoS involve board ranges of technologies, architecture and protocols. Network operators achieve end-to-end QoS by ensuring that elements applying consistent treatment to traffic flow as they travers the network.

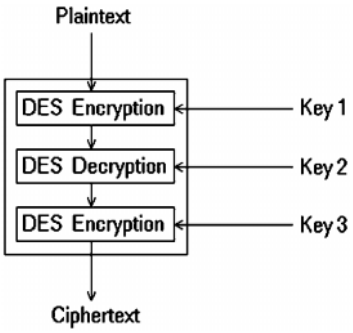
Why is QoS important? Today, networks traffic is highly diverse and each traffic type has unique requirement in terms of bandwidth, dealy, loss and availability. With the explosive growth of the internet, most network traffic today is IP-based. Having a single end-to-end transport protocol is beneficial because networking equipment becomes less complex to maintain, resulting in lower operational costs. This benefit, however is countered by the fact that IP is a connectionless protocol. I.e IP packets do not take a specific path as they travers the network. This results in unpredictable QoS in a best-effort network.

- QoS technologies play a crucial rol in a multiservice IP network.
- The greatest challenge for network operators today is to provide highly available IP networks.
- Some applications can compensate for small amounts of delay but once a certain amount is exceeded, the QoS becomes compromised.
- As long as the jitter is bounded, QoS can be maintained.
- Without applying QoS technologies, the traffic will experience unpredictable behavior.
- Interactive applications expect the network QoS to provide packets with the lowest possible delay, jitter and loss.

This document was created using SOLIDPDFTools To remove this message, purchase the product at www.SolidDocuments.com

- Timley applications expect network QoS to provide packets with a bounded amount of delay.
- Building a QoS enabled network requires a number of different QoS technologies.

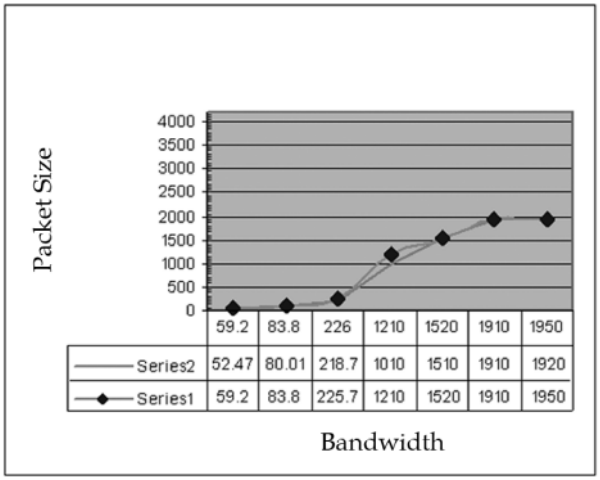
Concept of 3 DES:

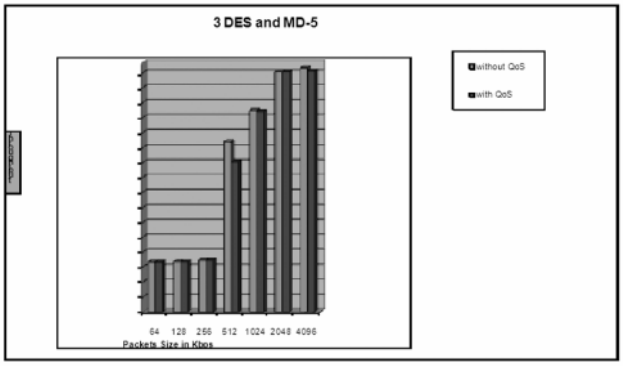


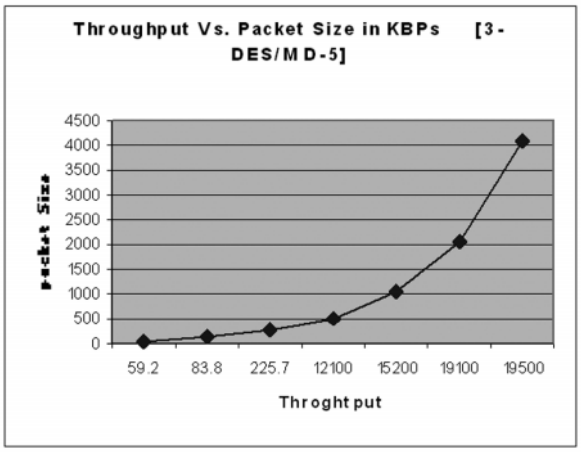
Triple DES was the answer to many of the shortcomings of DES. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES. However, even this more powerful version of DES may not be strong enough to protect data for very much longer. The DES algorithm itself has become obsolete and is in need of replacement. To this end the National Institute of Standards and Technology (NIST) is holding a competition to develop the Advanced Encryption Standard (AES) as a replacement for DES. Triple DES has been endorsed by NIST as a temporary standard to be used until the AES is finished sometime in 2001.The AES will be at least as strong as Triple DES and probably much faster. Many security systems will probably use both Triple DES and AES for at least the next five years. After that, AES may supplant Triple DES as the default algorithm on most systems if it lives up to its expectations. But Triple DES will be kept around for compatibility reasons for many years after that. So the useful lifetime of Triple DES is far from over, even with the AES near completion. For the foreseeable future Triple DES is an excellent and reliable choice for the security needs of highly sensitive information.

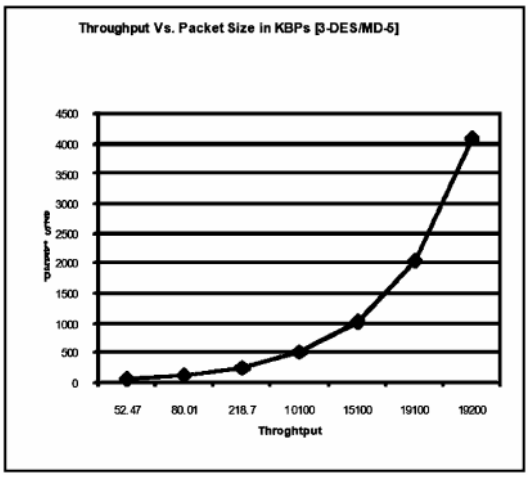
5. RESULT ANAYSIS

Packet Size in Kbps	*BW without QoS*	*With QoS*
64	59.2	52.47
128	83.8	80.01
256	225.7	218.7
512	12100	10100
1024	15200	15100
2048	19100	19100
4096	19500	19200









This document was created using SOLIDPDFTools To remove this message, purchase the product at www.SolidDocuments.com

CONCLUSION

QoS technologies are required for every type of network. From the observation it is clear that QoS provide effective bandwith while using diff. Encryption algorithm, After applying QoS, the throughput slightly vary but need arise for each multiplayer switched network design to include QoS for maintaining proper service of network. QoS also limits an attackers ability to impose or steal information, Although QoS cannot prevent theft of information.

REFERENCE

[1] M. Devargas, "Network Security", Manchester, England.: NCC Blackwell, 1993.

[2] B. Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C", NY.: John Wiley & Sons, 1994.

[3] Richard Froom, "Authorized Self –Study Guide–Building CISCO Multilayer Switched Networks [BCMSN], Cisco Press.

[4] Cynthia Irvine, Timothy Levin, "Quality of Security Service ".

[5] Mahmoud Mostafa, Christian Fraboul. "Q-ESP : a QoS - Compliant Secuirty Protocol to Enrich IPSec Framework".

[6] Timothy M. O'Neil, "Network based Quality of Service" White Paper by Polycom.

[7] Nortel Netwrok, "Introduction of Quality of Service [QoS]" White Paper.

[8] Partha Bhattacharya, "Security and Quality of Service Management.

[9] John McHugh, "Security and Quality of Service Interactions ".

[10] Klara Narhstedt, "Can Network QoS and Security Live in Symbiosis? ".

[11] S.D. Patil / Dr. AjayKumar "Network Based Quality of Service[QoS] for Various Traffic."

[12] S.D. Patil / Dr. AjayKumar, "Security and Quality of Service [QoS] Interactions ".

[13] Quality of Service in Multimedia Networks - QoS Elements, Realization of QoS, Network Scalability and Application LayerMulticasting. http://encyclopedia.jrank.org/ articles/pages/6874/Quality-of-Service-in-Multimedia-Networks.html#ixzz0hgBhmmf7.

This document was created using SOLIDPDFTools To remove this message, purchase the product at www.SolidDocuments.com