Laboratorio experimental para evaluación de tecnologías de Internet2

Raúl Rivera Rodríguez, Ma. Concepción Mendoza Díaz,
Raúl Tamayo Fernández*, Mario Farias-Elinos**, Azael Fernández Alcántara***
Dirección de Telemática, *Departamento de Redes, CICESE. **Escuela de Ingeniería Universidad La Salle,
***Universidad Nacional Autónoma de México
Km 107 Carretera Tijuana-Ensenada, Ensenada, B. C., México, C.P. 22860
Tel. +52 (646) 174-5050. Fax. +52 (646) 175-0597
rrivera@cicese.mx, comedi2001@yahoo,com, rtamayo@cicese.mx, elinos@ci.ulsa.mx

RESUMEN

En este documento se describen los aspectos técnicos del laboratorio de interoperabilidad de sistemas, a nivel de red, transporte y aplicación, instalado en la reunión de otoño de CUDI-2001, enfocándose en el análisis de desempeño al implementar esquemas de seguridad. Las pruebas realizadas entre los grupos de trabajo de Seguridad, Calidad de Servicio e IPv6 de CUDI arrojan resultados interesantes en el desempeño de los esquemas VPN con encriptación. Estos resultados servirán para determinar conclusiones en los aspectos de crecimiento y planificación de servicios en la dorsal de la red de CUDI. Para llevar al cabo lo anterior se conceptualizó, diseñó e instrumentó un escenario controlado para pruebas de IPSec, se demostró el funcionamiento de una VPN y conexión segura, así como su impacto en las aplicaciones multimedia. Y de esta forma contar con un esquema para evaluar los protocolos y aplicaciones utilizadas en Red CUDI con y sin servicios de seguridad y QoS.

I. INTRODUCCIÓN.

En apoyo a la iniciativa del Grupo Técnico de Internet 2 en CICESE para demostrar los alcances de las tecnologías en experimentación en vivo, el Comité para el Desarrollo de la Red llevó al cabo por primera vez, el proyecto de implementación de un Laboratorio de Interoperabilidad, en la Reunión de Otoño de CUDI en la ciudad de Guadalajara,, Jalisco.

La red que conformó el Laboratorio de Interoperabilidad contiene elementos para aplicar Calidad de Servicio, equipo para establecer videoconferencias con H.323, herramientas para trabajar con video por paquetes Multicast, conexión a Internet y a Internet2, más algunos segmentos con IPv6.

La coordinación de la implementación del Laboratorio fue responsabilidad del Grupo Técnico I2-CICESE, durante la cual se realizaron las siguientes actividades:

- Contacto con los responsables de los Grupos de Trabajo del CDR.
- Diseño del Laboratorio de Interoperabilidad en conjunto con los grupos de Calidad de Servicio y Seguridad.
- Organización del desarrollo de las actividades relativas al Laboratorio: instalación, desarrollo de pruebas, posters, tours, atención a los asistentes.
- Organización e implementación del laboratorio en conjunto con el comité local organizador de la UdeG.
- Elaboración de la memoria técnica.

II. DESCRIPCIÓN DEL LABORATORIO DE INTEROPERABILIDAD

La figura 1 muestra el diagrama de conexión de red que se implemento. Esta red consta de un acceso WAN que da conectividad a la dorsal de Internet2 de CUDI, un conmutador de core que une a las interfaces de WAN con los *gateways* de LAN. A continuación se describe brevemente la implementación que se realizo en cada grupo de trabajo (seguridad, QoS, e IPv6).

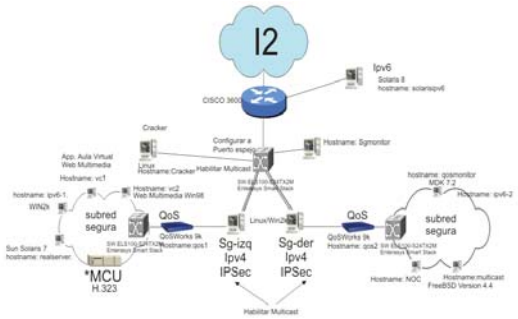

Figura 1. Laboratorio de Interoperabilidad de la Reunión de Otoño de CUDI'01.

ROC&C 2002 "C-20" PONENCIA RECOMENDADA POR EL CAPITULO DE COMUNICACIONES DEL IEEE SECCION MÉXICO Y PRESENTADA EN LA REUNION DE OTOÑO DE COMUNICACIONES, COMPUTACIÓN Y ELECTRÓNICA ROC&C 2002 ACAPULCO, GRO. 1 AL 6 DE OCTUBRE DEL 2002

Grupo de trabajo de Seguridad.

Como resultado de la investigación sobre la Seguridad para el Protocolo IP (IPSec) [Mendoza, 2002], se propuso la implementación de una VPN, se experimentó con implementaciones del tipo BITS (Bump In The Stack), en diferentes Sistemas Operativos. Se eligieron dos sistemas diferentes, populares y utilizados en el entorno de Internet2: MS-Windows2000, para probar conexiones seguras con IPSec para IPv6; y Linux en su distribución Slackware 8, para la VPN con IPv4.

Las conexiones seguras *host-to-host* fueron probadas sobre MS-Windows2000 y su versión experimental IPSec6 para IPv6, y la VPN creada a través de FreeS/WAN1.91 con IPv4 sobre Linux. Los *Gateways* de Seguridad fueron instrumentados en GNU/Linux en su variante Slackware con el proyecto FreeS/WAN [FreeS/WAN].

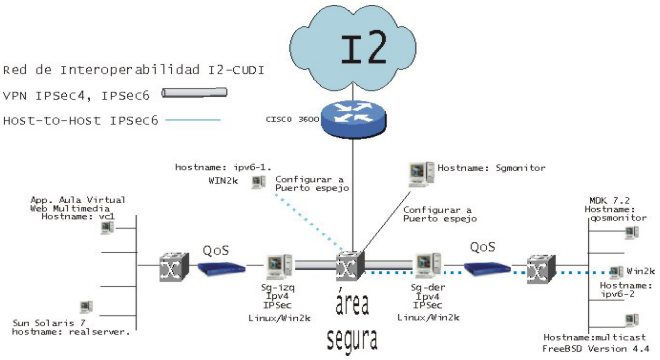

Figura 2. Escenario de pruebas de IPSec diseñado para la Reunión de Otoño de CUDI 2001.

Se creó una VPN con dos gateways de seguridad instrumentando IPSec en modo túnel, con IPv4, creando asociaciones de seguridad para las subredes izquierda y derecha de la siguiente forma: se aplicó ESP, manejo de llaves manual, SPI 200, y se generaron para cada SG, llaves para autenticación y para encriptación. El algoritmo de encriptación es 3DES-MD5-96. Adicionalmente, se estableció una conexión segura con IPSec6 en modo transporte, IPv6, políticas de seguridad para todo el tráfico y autenticación como servicio de seguridad, también fueron complementadas.

La figura 2 resalta las configuraciones de IPSec. La VPN se resalta con un tubo grueso entre los gateways de seguridad centrales, y la conexión segura se resalta con una línea punteada entre un host de la subred central y un host de la subred derecha.

Grupo de Trabajo de Calidad de Servicio.

Para la parte de Calidad de Servicio se implementó una aproximación de lo que seria QoS extremo-extremo desde el punto de viste de nodo de acceso, como se muestra en la figura 3. Aquí se muestra el ambiente de QoS aplicado en los nodos de acceso teniendo un control sobre los flujos de las aplicaciones críticas. Para las pruebas se aplicó calidad de servicio a las aplicaciones como H.323, video en demanda y otras como educación a distancia usando aplicaciones del Mbone Tools, como el sistema SDR de Multicast. También se realizó una prueba de video en demanda a 450 Kbps aplicando QoS en el nodo de CICESE, en Ensenada, B.C. a través de Internet2.

Cabe señalar que durante las pruebas de VPN con encriptación e IPv6, los equipos de QoS estuvieron funcionando normalmente.

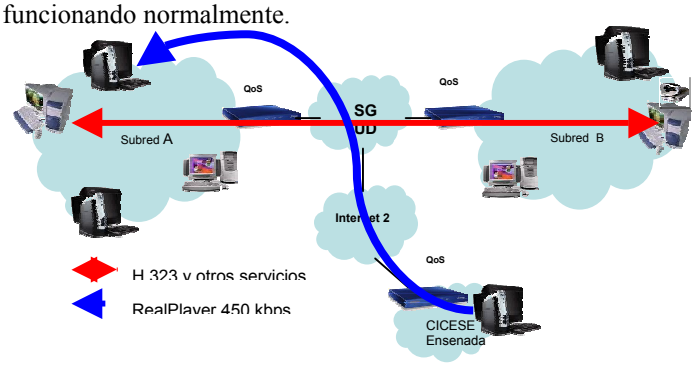

Figura 3. Escenario de pruebas de QoS + IPSec para la Reunión de Otoño de CUDI 2001.

Grupo de Trabajo de IPv6.

Utilizando la maqueta de pruebas de la figura 4, se configuró en primera instancia el enrutador Cisco 3600 para dar salida con IPv6 por Internet2. Para lo cual se habilitó IPv6 en las interfaces del equipo, se configuró un túnel de IPv6 sobre IPv4 con BGP4+ entre este enrutador y el de Backbone de Internet2 de la ciudad de México, que hasta entonces era el único con IOS para IPv6, utilizando el prefijo 2001:0448:3:1::/64 que es parte del asignado a CUDI, el 2001:0448:3::/48 [6Bone]. Así mismo se habilitó la autoconfiguración de las direcciones para todas las PCs y estaciones de trabajo que tuvieran soporte para IPv6.

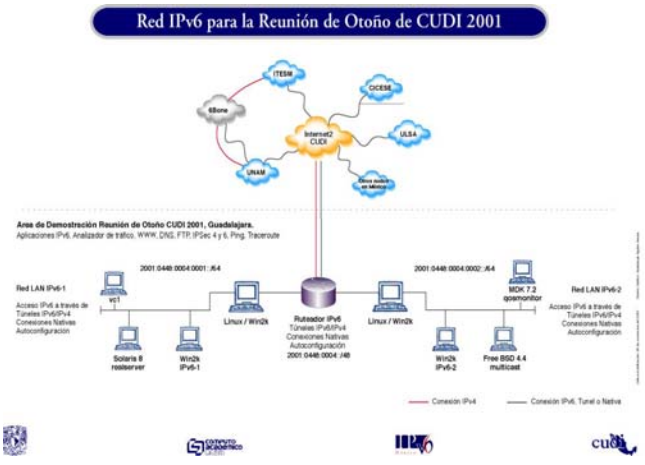

Figura 4. Red IPv6 utilizada durante la Reunión de Otoño de CUDI 2001

En dos de las computadoras con Windows2000 se instaló el Stack de IPv6, el MSR 1.4 [MS-IPv6], se configuró un túnel de IPv6 de sobre IPv4 entre ambas, al

estar en segmentos diferentes, utilizando las direcciones 2001:0448:3:1::15 y 2001:0448:3:1::34 respectivamente y automatizando la configuración con la creación de un script. A continuación se muestran los resultados de las pruebas realizadas.

III. Desarrollo de pruebas.

El laboratorio entregó resultados muy interesantes, se tuvo la oportunidad de probar protocolos como multicast, H.323 y otros, con y sin servicios de seguridad, las pruebas realizadas y los resultados se describen a detalle posteriormente. Se generó tráfico *multicast*, video por paquetes (H.323), entre otros. Las muestras fueron obtenidas con la VPN desactivada, 100 muestras de tres tamaños de paquete distintos: 64, 1024 y 2024 bytes, y con la VPN activada, 100 muestras con los mismos tamaños de paquete. El tamaño de paquete es importante para observar el comportamiento por fragmentación, al manejar datos, voz y video, más esquemas de encapsulamiento que aumentan la carga útil de un paquete y obligan su división para ser transmitidos. Se transmitieron paquetes pequeños de 64 bytes, paquetes de 1024 bytes (la unidad máxima de transmisión (MTU) en Ethernet es 1518 bytes) y paquetes grandes de 2024 bytes.

En todos los casos, se utilizaron herramientas de análisis de tráfico, para obtener retardos y *throughput*, con ello se calculó el *jitter* para evaluar el sistema, con y sin servicios de seguridad, para definir si los valores resultantes cumplen los valores permitidos de parámetros de desempeño para los servicios sensibles del tiempo: un retardo de 400ms y *jitter* de 20ms para voz, mismo retardo y 30ms de *jitter* para video [Cruz, 2001] (ver Tabla I).

Discusión de resultados.

Los resultados que se analizarán a continuación, arrojan conclusiones interesantes, en contra de lo que se hubiera esperado en un principio sobre la degradación del sistema al aplicar servicios de seguridad. Se encontraron resultados donde los mecanismos de *buffering* en un *gateway* de seguridad facilitan el control de los paquetes e impactan de forma positiva los servicios sensibles del tiempo de transmisión.

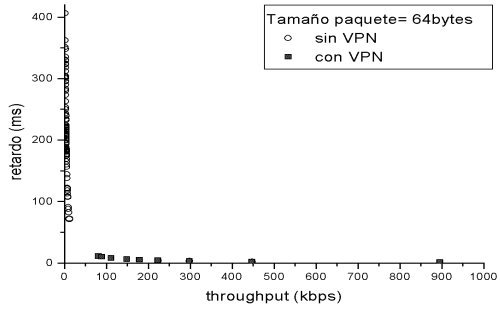

Figura 7. Gráfica de throughput vs retardo para la transmisión de paquetes de 64bytes con y sin servicios de seguridad.

De acuerdo a la figura anterior, al transmitir paquetes sin la VPN, los retardos fueron altos, alcanzando un máximo de 406 ms con un caudal eficaz de 2.2 Kbps y un mínimo retardo de 82 ms, con un caudal eficaz de 10.92 Kbps, es decir, una comunicación bastante mala. El retardo máximo para la calidad en transmisión de voz y video es de 400ms [Cruz, 2001], por lo que en este esquema se rebasa. Esta situación fue observable en las aplicaciones multimedia que se estaban ejecutando , al activar la VPN el cambio fue totalmente notorio, el aumento en la calidad del servicio fue inmediato y sorprendente, al analizar los datos obtenidos, se ratificó el comportamiento observado, con servicios de seguridad, se tuvo un máximo retardo de 10 ms con un caudal eficaz de 89.6 Kbps, y un mínimo retardo de 1 ms alcanzando un caudal eficaz de 896 Kbps. Es decir, muy por debajo de los límites permitidos para voz, video y datos que se muestran en la tabla I [Cruz, 2001].

Tabla I. Valores permitidos de parámetros de desempeño para diferentes servicios.

Servicio	Retardo	Variación en el retardo
Voz	400ms	20ms
Video	400ms	30ms
Datos	1400ms	--

Este comportamiento se atribuye a la intervención de los *gateways* de seguridad sobre cada paquete transmitido y recibido, al dar un tratamiento especial para insertar encabezados de autenticación y secuencia de los mismos. Este mecanismo mejoró la recepción reflejada en la disminución de retardos que además se mantuvieron estables produciendo un *jitter* también bajo.

Uno de los elementos que da mayor información para evaluar el comportamiento de una red, es la variación del retardo (*jitter*). Los datos estadísticos obtenidos, en base a las variaciones del retardo para cada uno de los tres muestreos realizados se encuentran en la tabla II, de donde las variaciones son notables entre los datos sin la VPN activa con respecto a los datos con la VPN activa. Variaciones que respaldan lo observado durante las pruebas en las pantallas de aplicación, al mejorarse de forma evidente el video y el audio, servicios que son sensibles al tiempo. El comportamiento se mantuvo para los tres escenarios de prueba, en cada caso las prestaciones del sistema con la VPN activada, fueron por mucho superiores a los obtenidos sin la VPN activada.

Tabla II. Determinación de los momentos centrales del *jitter*.

Eventos	Media	Desviación Estándar	Área
Tamaño paquete: 64B			
Sin VPN	65.88855		1133.03484
Con VPN	0.00805	99.42132	9.44581
		0.06014	
Tamaño paquete: 1024B			
Sin VPN	19.66815	96.43093	2161.60285
Con VPN	0.37322	1.17755	33.53168

Tamaño paquete: 2024B Sin VPN Con VPN	12.44351 2.07721	42.36587 4.8416	1200.58529 51.5161

Para el caso de paquetes de 64bytes, el histograma resultante del *jitter* calculado para el muestreo sin la VPN se muestra en la figura 8, el comportamiento del *jitter* con la VPN activa, se encuentra en la figura 9. La media sin la VPN fue de 65 ms en contraste con 0.008 ms con la VPN, la desviación estándar y el área de la curva establecieron diferencias muy fuertes, los valores sin la VPN muy dispersos con variaciones muy altas, lo que indica una comunicación degradada.

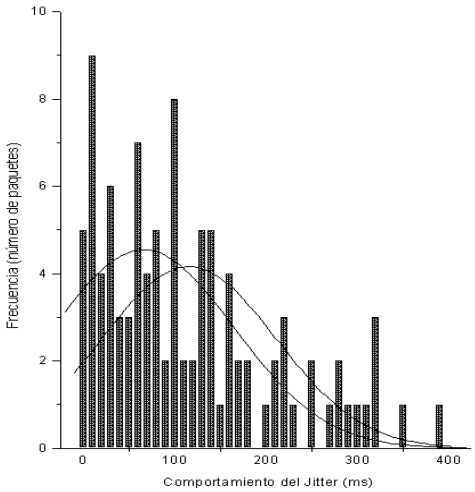

Figura 8. Histograma de la variación de retardo sin servicios de seguridad para paquetes de 64bytes

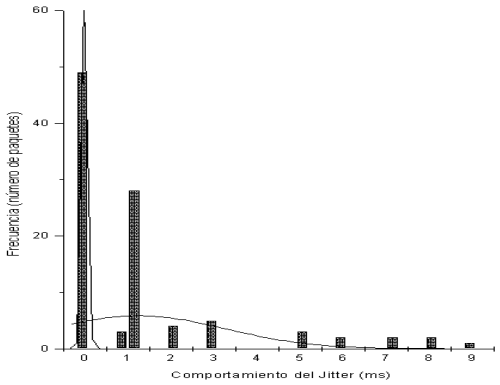

Figura 9. Histograma de la variación de retardo con servicios de seguridad para paquetes de 64bytes.

El siguiente muestreo se realizó con paquetes de 1024 bytes, mismas 100 muestras, mismo tráfico generado en la red, con y sin servicios de seguridad de la VPN. La figura 10 muestra la gráfica *throughput* vs retardo, donde el caudal eficaz sin VPN fue mucho mejor que en el caso anterior, sin embargo, el contraste se mantuvo, el máximo retardo sin la VPN fue de 484 ms con un caudal eficaz de 20.69 Kpbs, un mínimo retardo de 7ms alcanzando un caudal eficaz de 2Mbps. Con la VPN el máximo retardo fue 18 ms alcanzando un caudal eficaz de 352Kpbs, y un retardo mínimo de 1 ms con un caudal eficaz de 896Kpbs, el máximo caudal eficaz fue de 5.8Mb (casi el 60% de utilización) con un retardo de 2 ms.

La figura 11 muestra el histograma de la variación del retardo sin VPN y la figura 12 el histograma de la variación del retardo con la VPN activada.

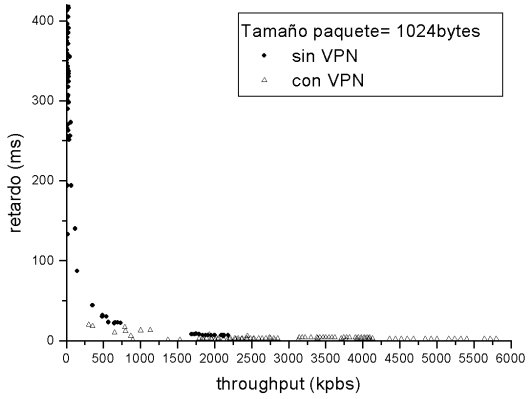

Figura 10. Gráfica de throughput vs retardo para la transmisión de paquetes de 1024bytes con y sin servicios de seguridad.

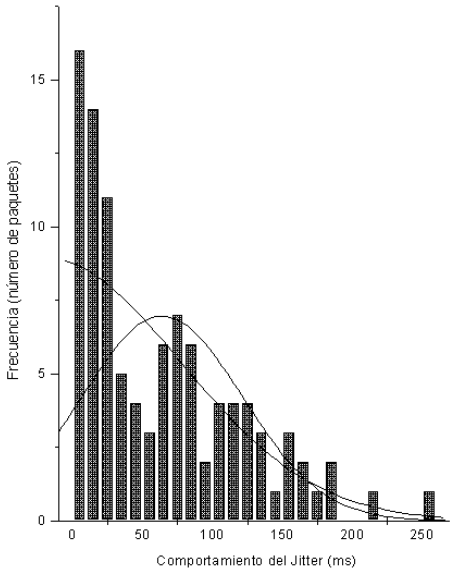

Figura 11. Histograma de la variación de retardo sin servicios de seguridad para paquetes de 1024bytes.

El comportamiento del *jitter* se mantuvo en este

escenario, de nuevo la mejoría de la comunicación fue visible al habilitar los servicios de seguridad de la VPN, los datos estadísticos marcan de nuevo la dispersión de los datos, alta variación del *jitter* en el muestreo sin la VPN, y valores estables y buenos en el muestreo con la VPN.

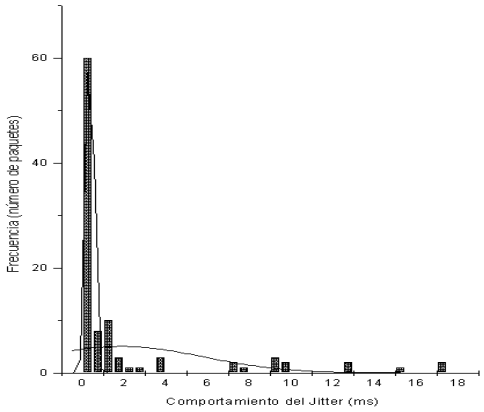

Figura 12. Histograma de la variación de retardo con servicios de seguridad para paquetes de 1024bytes.

El último muestreo se aplicó con paquetes de 2024bytes, paquetes grandes que rebasan el MTU para provocar fragmentación, bajo las mismas circunstancias que los muestreos anteriores, con y sin servicios de seguridad. La figura 13 muestra la gráfica obtenida de *throughput* vs retardo, donde también se observa un comportamiento similar a los casos anteriores, retardos y *jitter* altos, poco caudal eficaz para la red sin servicios de seguridad, y retardos pequeños y variaciones mínimas del retardo con caudal eficaz casi al 60% de utilización al tener los servicios de seguridad activos. En la figura 14 se muestra el histograma del *jitter* sin habilitar la VPN , donde se muestra de nuevo un comportamiento similar a los casos anteriores, un área amplia de la envolvente con una media de 12.44 ms.

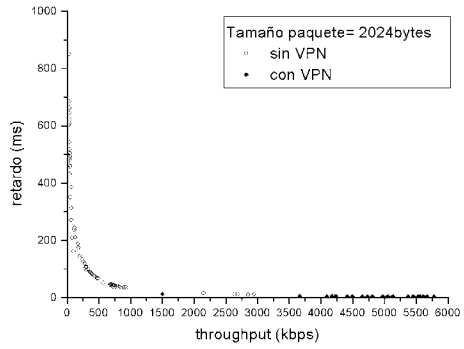

Figura 13. Gráfica de throughput vs retardo para la transmisión de paquetesde 2024bytes con y sin servicios de seguridad.

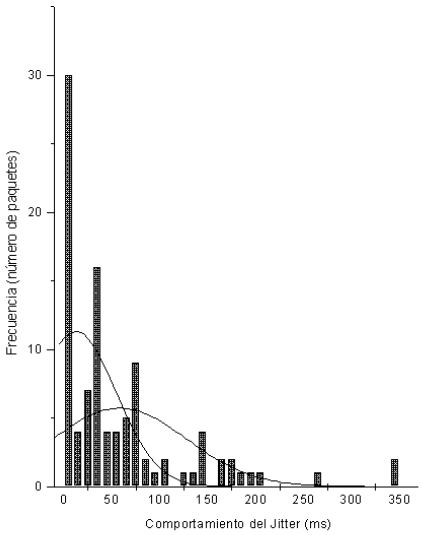

Figura 14. Histograma de la variación de retardo sin servicios de seguridad para paquetes de 2024bytes.

En la figura 15 se muestra el histograma del *jitter* con la VPN activada, en este caso la variación es muy pequeña con una media de 2 ms. Es importante mencionar que en este escenario el sistema llegó a un punto de saturación, debido al tamaño forzado de los paquetes superior al máximo definido para una red de este tipo, por lo que el número de muestras fue inferior al de los casos anteriores.

El comportamiento se mantuvo para los tres escenarios de prueba, en cada caso las prestaciones del sistema con la VPN activada, fueron por mucho superiores a los obtenidos sin la VPN activada.

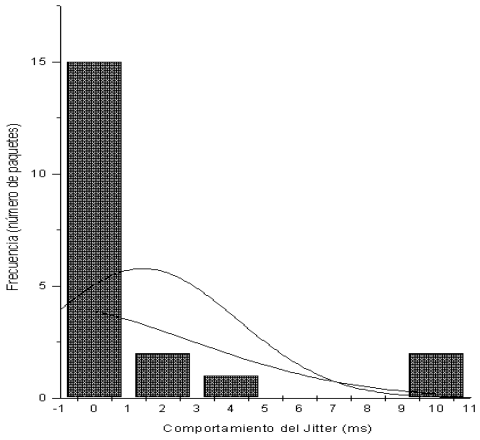

Figura 15. Histograma de la variación de retardo con servicios de seguridad para paquetes de 2024bytes.

IV. CONCLUSIONES.

Algunos de los resultados obtenidos fueron sorprendentes, comúnmente se considera que aplicar servicios de seguridad implica sacrificar prestaciones de la red o de un sistema, ya que los métodos de seguridad implican costo de procesamiento, de sobreflujo en la red, relleno, etc. Para el caso de servicios sensibles al tiempo, resulta interesante conocer que los mecanismos de *buffering* que aplica un *gateway* de seguridad para autenticar y ordenar paquetes cifrados impacta de forma positiva a aplicaciones multimedia. Considerando las cotas para servicios sensibles de tiempo mostradas en la tabla I, en los casos sin la VPN, donde los retardos fueron altos y la media del *jitter* fue arriba de los 20ms, se encuentran en la cota máxima de calidad de servicio para voz, y cerca de la cota máxima de 30ms para video. En los casos con la VPN, los parámetros de desempeño tuvieron valores mínimos con prestaciones excelentes para la transmisión de video y voz. En la tabla III se muestra un resumen de las estadísticas obtenidas.

El análisis de tráfico resaltó las deficiencias de IP con respecto a seguridad, la transmisión de datos se realiza sin considerar que puede haber "un hombre en el medio". Los esfuerzos a nivel de aplicaciones para cifrar sus datos son importantes y funcionales, aunque IPSec resulta ser un excelente complemento para todas aquellas aplicaciones que no integran servicios de seguridad por sí mismas.

Se ha considerado un escenario real de pruebas con las ventajas inherentes de experimentar en un ambiente real, e interactuar directamente con otras nuevas tecnologías, los resultados obtenidos han contribuido a la consideración de IPSec, como una alternativa para brindar servicios de seguridad en la Internet de siguiente generación en nuestro país.

Contrario a lo que comúnmente se maneja, una VPN no es solamente una red virtual (conmutada), es además privada, no representa una solución completa, y no brinda protección total a una red, una VPN protege únicamente el canal por donde transita la información de un extremo a otro de la VPN, si uno de los extremos de la VPN o de una conexión segura host-to-host se compromete, se perdió la protección. Más aún, una VPN o conexión segura no brinda ninguna protección con respecto a intrusiones a una computadora, es decir, el hecho que se apliquen VPN o conexiones seguras no sustituye el esfuerzo que debe hacerse por instrumentar mecanismos de seguridad en sistemas, sobre todo si la implementación de IPSec es del tipo BITS en sistema operativo.

V. BIBLIOGRAFÍA.

6Bone, Página de la base de datos sobre sitios de IPv6. (http://www.cs-ipv6.lancs.ac.uk/ipv6/6Bone/Whois).

Cruz, Patiño Héctor Raúl. *Análisis y modelado de mecanismos para la implementación de redes con calidad de servicio*. Tesis de Maestría, Departamento de Electrónica y Telecomunicaciones, CICESE. Agosto 2001.

FreeS/WAN, Free Security Wide Area Network (www.freeswan.org).

Linkview, Página de Wavetek Wandel Goltermann (www.wavetek.com).

Mendoza, Díaz María Concepción. Protocolos de Seguridad e Instrumentación de IPSec en Escenarios Experimentales en Internet 2 en México. Tesis de Maestría, Departamento de Ciencias de la Computación, CICESE. Enero 2002.

MS-IPv6, Página de la implementación de IPv6 de Microsoft Research: (research.microsoft.com/msripv6).

Sitios-de-grupos-de-Trabajo-I2, http://www.cudi.edu.mx/informacion_tecnica/grupos_trabajo.html

CURRICULUM VITAE

Raúl Rivera Rodríguez. Recibió su título en Tecnológico de Sonora (ITSON) de la carrera de Ingeniero en Electrónica en 1994, y de Maestro en Ciencias en Electrónica y Telecomunicaciones por parte del Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE) en 1997. Desde entonces trabaja como Responsable del Área de Gestión de Redes de Telecomunicaciones de la Dirección de Telemática de CICESE. También es profesor del Departamento de Electrónica y Telecomunicaciones del CICESE. Y actualmente coordinador del grupo de trabajo de QoS de CUDI-Internet2.

Raúl Tamayo Fernández. Recibió su título de Ingeniero en Electrónica por parte de la Universidad Autónoma de Baja California (UABC) en 1994, y de Maestro en Ciencias en Electrónica y Telecomunicaciones por parte del Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE) en 1997. Desde entonces trabaja como Responsable del Área de Planeación en el Departamento de Redes de la Dirección de Telemática de CICESE. También es profesor por asignatura en la UABC y en el Departamento de Electrónica y Telecomunicaciones de CICESE.

Concepción Mendoza Díaz. Recibió su titulo de Licenciado en Ciencias de la Computación en la Universidad Autónoma de Baja California (UABC) en 1994, y de Maestro en Ciencias en Ciencias de la Computación por parte del Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE) en 2002. Hasta abril de 2002 colaboró en la Dirección de Telemática como coordinadora del Grupo de Seguridad de Red-CICESE.

Mario Farias-Elinos obtiene el titulo de Ingeniero en Cibernetica y en Sistemas Computacionales por la Universidad La Salle (ULSA) en 1996 y el grado de Maestro en Ciencias en la Especialidad de Ingenier'ia El'ectrica por el Centro de Investigaci'on y de Estudios Avanzados (CINVESTAV-IPN). Es miembro titular del Laboratorio de Investigaci'on y Desarrollo de Tecnolog'ia Avanzada (LIDETEA) e Investigador de la Escuela de Ingenier'ia de la ULSA desde 1997. Sus 'areas de investigaci'on son: Seguridad en C'omputo, Procesamiento de Im'agenes y computo distribuido y paralelo. Actualmente es candidato al grado de Doctor en Ciencias en la Especialidad de Ingenier'ia Electrica por el CINVESTAV y Coordinador Nacional del Grupo de Seguridad de Internet-2.