SECURE VoIP NETWORK MENGGUNAKAN PROTOKOL SRTP

Fauzar Amin, Ir. Muhammad Husni, M.Kom
Jurusan Teknik Informatika – FTIF, Institut Teknologi Sepuluh Nopember
Kampus ITS, Sukolilo, Surabaya – 60111
E-mail : fauzaramin@yahoo.com

Abstrak : *Teknologi Voice Over Internet Protocol (VoIP) merupakan suatu terobosan dalam komunikasi data. Namun demikian faktor keamanan data pada VoIP masih rentan terhadap kemungkinan penyalahgunaan (abuse), hacking, data-sniffing dan berbagai macam ancaman lainnya.*

Pada tugas akhir ini telah dicapai suatu system yang dapat digunakan untuk mengamankan komunikasi VoIP. Dengan menggunakan teknologi Secure Real Time Protocol (SRTP)) dapat digunakan untuk mengamankan transfer media signalling RTP yang digunakan, serta dengan metode kriptografi pada SRTP, VoIP dapat mengacak suara yang akan dikirimkan sehingga tidak dapat disadap.

Dengan eksperimen yang telah dilakukan, penggunaan sistem SRTP pada VoIP terdapat korelasi terhadap kualitas suara berdasarkan parameter QoS (Quality of Service) dengan penggunaan sistem RTP yang biasa digunakan pada teknologi VoIP.

Kata Kunci : *VoIP, RTP, SRTP, Secure, QoS*

1. PENDAHULUAN

VoIP (*Voice over Internet Protocol*) atau dapat juga disebut sebagai Telepon Internet (*Internet Telephony*) merupakan salah satu terobosan dalam berkomunikasi secara luas dengan biaya yang lebih murah. VoIP merupakan suatu metode digitalisasi data suara (*voice*) kedalam paket-paket data untuk ditransmisikan melalui *packet-switch IP network.*

SIP (*Session Initiation Protocol*) merupakan protokol yang berada pada layer aplikasi yang mendefinisikan proses awal, pengubahan, dan pegakhiran (pemutusan) suatu sesi komunikasi multimedia. Protokol RTP (*Real Time Protocol*) merupakan media *signaling* komunikasi multimedia tersebut yang berupa suara dan video. Paket SIP (RTP) biasanya di kirim melalui protokol UDP (*User Datagram Protocol*) dan TCP (*Transmission Control Protocol*). Karena kebanyakan lalu lintas paket yang dikirimkan melalui VoIP tidak dienkripsi, siapapun yang terkoneksi ke jaringan akan dapat men-*capture* data. Penangkapan/pengambilan *streaming* suara dan men-*decode* media *signaling* dapat dilakukan dengan mudah oleh *Eavesdropper*/penyusup dengan *tool sniffing* yang ada untuk merekam pembicaraan suara dalam jaringan VoIP yang tidak aman.

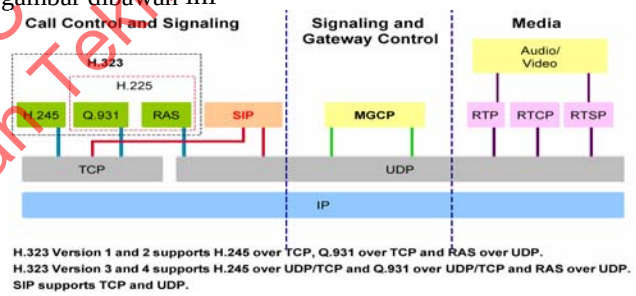
Salah satu cara menangani serangan/penyadapan pada jaringan VoIP ini adalah dengan menggunakan mekanisme enkripsi. Protokol SRTP (*Secure Real Time Protocol*) salah satu mekanisme enkripsi yang dapat mengenkripsi media *streaming* suara dan menyediakan *fiture* keamanan pada RTP untuk menambah kerahasiaan, otorisasi pesan, dan proteksi terhadap *replay* pesan yang dikirim.

Pada Tugas Akhir ini dilakukan perancangan server VoIP dengan menggunakan protokol SRTP sebagai media komunikasi enkripsi masalah keamanan data *streaming* suara yang dikirim *via* jaringan VoIP, beserta *tool* pendukung terhadap protokol tersebut. Untuk menguji kemampuan keamanan server tersebut juga dirancang metode penyadapan yang dapat dilakukan *eavedropper*

2. TEORI PENUNJANG

2.1 Sistem SIP

Tinjauan tentang SIP dapat digambarkan seperti gambar dibawah ini



Gambar 2. 1 SIP Dalam Aplikasi

Keterangan:

a. RTP (*Real Time Protocol*)

Protokol RTP menyediakan transfer media secara *real-time* pada jaringan paket. Protokol RTP mengunakan Protokol UDP dan *header* RTP mengandung informasi kode bit yang spesifik pada tiap paket yang dikirimkan; hal ini membantu penerima untuk melakukan antisipasi jika terjadi paket yang hilang.

b. RTCP (*Real Time Control Protokol*)

Protokol RTCP merupakan *protokol* yang mengendalikan transfer media. *Protokol* ini bekerja sama dengan *protokol* RTP (untuk memudahkan pemahaman).

c. User Datagram Protocol (UDP)

UDP yang merupakan salah satu *protocol* utama diatas IP merupakan *transport protocol* yang lebih sederhana dibandingkan dengan TCP. UDP digunakan untuk situasi yang tidak mementingkan mekanisme reliabilitas

2.2 Keamanan Jaringan VoiP

Lalu lintas data dalam jaringan VoIP dapat diklasifikasikan menjadi *call control, call signalling dan media communication*. Selain VoIP tergantung dari protokol dan aturan yang ada, komunikasi VoIP dapat menggunakan satu atau beberapa saluran/*layer* transpor. Saluran itu adalah koneksi TCP/UDP antara 2 *network* elemen. Dari titik pandang keamanan, seluruh koneksi tersebut membutuhkan pengamanan terhadap saluran yang digunakan. Contoh : otorisasi dan enkripsi. Beberapa mekanisme pengamanan terhadap jaringan VoIP adalah sebagai berikut :

- Otorisasi dan otentikasi
  VoIP call *signalling* dan *call control* dapat diamankan dengan mengimplementasikan metode otorisasi dan otentikasi. Otorisasi mengandung pengertian bahwa komponen VoIP dapat dikonfigurasikan dengan cara mengizinkan grup IP *address* yang dipilih yang dapat mengakses jaringan VoIP. Mekanisme ini melindungi dari serangan *Denial-of-Service(DoS)*. Otentikasi membutuhkan komunikasi *device* VoIP terlebih dahulu sebelum terhubung untuk memulai komunikasi sebenarnya(pembicaraan). Otentikasi ini berdasarkan pada berbagi/*shared* kerahasiaan pada masing-masing yang ingin komunikasi atau yang disebut dengan prioritas, hal ini membuat sulit seorang penyerang untuk menyamarkan identitas.
- *Transport Layer Security* (TLS)
  TLS dapat menyediakan keamanan saluran komunikasi antara dua komunikasi yang terjadi. Tujuan utama protokol TLS ini adalah menyediakan privasi dan data *integrity* antara dua aplikasi komunikasi. TLS mengizinkan aplikasi *client/server* untuk berkomunikasi dalam jalur yang didesain untuk melindungi dari *eavesdropper*, perusakan atau pemalsuan paket pesan yang dikirim. Mekanisme secure komunikasi yang berdasarkan *shared* kerahasiaan yang hanya diketahui oleh *server* dan *client* membuat kesulitan dan mustahil *eavesdropper* untuk melihat, memanipulasi atau me-*replay* pertukaran pesan.
- Media *Encryption* (SRTP)
  Media komunikasi dapat juga diamankan dengan menerapkan beberapa mekanisme enkripsi. Telepon VoIP dapat menenkripsi *audio stream* melalui SRTP (*Secure Real Time Protocol*). SRTP adalah bagian pengamanan terhadap protokol RTP yang menambahkan kerahasiaan, otentikasi pesan, dan proteksi *replay* ke protokol tersebut. SRTP sangat ideal untuk memproteksi *voice* yang melewati jalur IP karena SRTP berhubungan dengan header paket VoIP dan tidak berefek pada *Quality-of-Service* IP. SRTP membuat *key stream* yang unik untuk tiap paket RTP, sehingga mustahil bagi *eavesdropper* untuk mengambil RTP *stream* asli dari enkripsi SRTP *stream*. SRTP juga menyediakan proteksi terhadap *replay* data multimedia. Seandainya tidak ada proteksi *replay* maka dapat terjadi manipulasi data dalam pengiriman *voice* pada aplikasi yaitu kata "*yes*" menjadi kata "*no*". SRTP menghasilkan *throughput* yang tinggi dan ukuran frame yang rendah dengan menggunakan *chiper stream* yang cepat untuk enkripsi. [1]

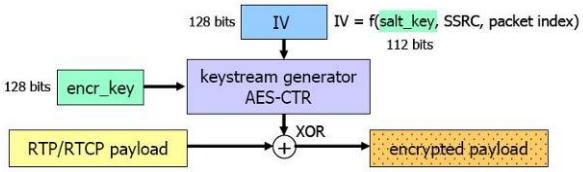
  Tujuan utama SRTP adalah
  - Sebagai pertimbangan keamanan VoIP
  - Privasi RTP *payload*.
  - Proteksi integritas terhadap seluruh paket RTP, termasuk proteksi *replay* paket RTP
  - Otentikasi terhadap *header*, *payload*, perluasan *header*
  - Mencegah terjadinya *DoS*

2.3 *Secure Real Time Protocol (SRTP)*

SRTP adalah profil bagi protokol RTP, yang bertujuan menyediakan enkripsi, otentikasi pesan, integritas dan juga proteksi *replay* ke data RTP dalam aplikasi *unicast* dan *multicast*. SRTP dikembangkan oleh team ahli IP protokol dan *cryptographic* dari Cisco dan Ericsson yaitu David Oran, Daid McGrew, Mark Baugher, Mats Naslund, Elisabetta Carrara, Karl Norman, dan Rolf Blom. SRTP di publikasikan oleh IETF bulan Maret 2004 dalam RFC 3711.[1]

2.4 Aliran Data *Enkripsi* SRTP

Enkripsi dan deskripsi aliran data oleh SRTP menggunakan standar *chiper* yaitu AES. Dimana AES ini menggunakan *counter mode* yang dinamakan *Segmented Integer Counter Mode* (SICM) yang melakukan akses *random* terhadap blok AES atau dengan kata lain memungkinkan penerima untuk memproses paket secara *random*. AES-SICM ini berjalan dalam *default* algortima enkripsi yaitu panjang *key* enkripsinya 128 bit. [2]

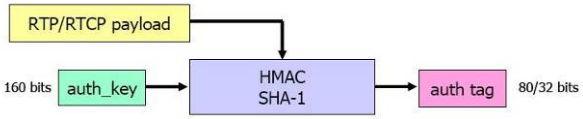


Gambar 2. 2 Enkripsi Menggunakan AES-Counter Mode

2.5 Otentikasi, Integritas dan Proteksi Replay

Algoritma enkripsi yang ada dipenjelasan atas tidak dapat mengamankan integritas paket dengan sendiri. SRTP menggunakan algoritma HMAC-SHA1 untuk memproteksi integritas otentikasi paket. Tanpa algoritma ini penyerang dapat memalsukan isi paket dan mengirimkan *replay* datanya kembali kepada pengirim. Algoritma HMAC-SHA1 mempunyai cara kerja dimana algoritma ini akan mengecek keaslian paket yang dikirimkan dengan terlebih dahulu melakukan pemeriksaan terhadap paket *header* yang ada pada data yang dikirimkan sebelumnya, sehingga jika

sama maka data akan diterima. Maka penyerang tidak akan dapat melakukan *replay* dengan data palsu.[2]

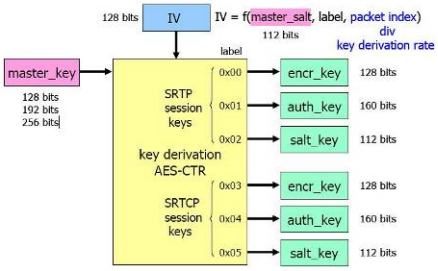


Gambar 2. 3 Otentikasi Menggunakan HMAC-SHA-1

2.6 *Key Derivation*

Fungsi *key derivation* yang terdapat dalam SRTP digunakan untuk menghasilkan key yang berbeda untuk digunakan dalam kontek *crypto*(enkripsi *key* dan *salt key* SRTP juga *key* otentikasi SRTP) dari satu master key dalam jalur keamanan *cryptography*. Dengan demikian, protokol manajemen *key* membutuhkan hanya satu *master key*, sedangkan *key session* dihasilkan dengan menerapkan *key derivation*.

Fungsi aplikasi *key derivation* yang dilakukan secara periodik menghasilkan manfaat keamanan yang besar. Hal ini dapat mencegah para penyerang untuk mengumpulkan enkripsi *chipertext* yang banyak dengan satu *key session*.[2]



Gambar 2. 4 *Session Key Derivation*

2.7 Parameter QoS VoIP

QoS yang diterapkan pada jaringan VoIP memiliki parameter yang menjadi ukuran kualitas layanan VoIP, yaitu antara lain [3]:

1. *End to end delay*

Didefinisikan sebagai penundaan yang mengkibatkan keterlambatan paket datang ke penerima. Perhitungan waktu tunda ini dimulai sejak informasi suara keluar dari mulut pengirim sampai ke telinga pendengar.

Dalam Tugas Akhir ini *end to end delay* didapatkan dengan menggunakan persamaan:

End to end delay = packetization delay + network delay

Packetization delay atau *process delay* tergantung dari *codec* yang digunakan, untuk G711 nilainya 0.125ms. Sedangkan *network delay* atau *transmission delay* didapat dari *round trip delay* yang diperoleh pada saat pengukuran [4].

2. *Jitter*

Merupakan perbedaan waktu kedatangan dari suatu paket ke penerima dengan waktu yang diharapkan. Paket VoIP akan dikirim ke penerima setiap interval waktu tertentu dan seharusnya akan diterima juga dalam setiap waktu tertentu tapi kenyataanya waktu kedatangan paket tidak sama. Jitter dapat menyebabkan sampling di sisi penerima menjadi tidak tepat sasaran sehingga informasi menjadi rusak. Jitter dapat diatasi dengan melakukan *buffering* (*jitter buffer*) atau penahanan paket sementara, yaitu paket berikutnya tidak dikirimkan sebelum paket pertama tiba di tujuan. Akan tetapi dengan adanya jitter buffer akan menambah jumlah dari *end to end delay*.

3. *Packet Loss*

Merupakan hilangnya paket dalam jaringan yang disebabkan faktor antrian (*queue*) yang melebihi batas waktu yang ditentukan dan atau ukuran paket yang terlalu besar sehingga tidak mungkin ditransmisikan dalam jaringan yang kecepatannya rendah.

Tabel 2.1 *Performance Standard* [5]

Grade	Delay (ms)	Jitter (ms)	Packet Loss (%)
Memuaskan	0-150	0-20	0-0.5
Dapat diterima	150-300	20-50	0.5-1.5
Jelek	>300	>50	>1.5

2.8 *Mean Opinion Score* (MOS)

MOS memberikan indikasi numerik dari kualitas suara secara subyektif. MOS diekspresikan sebagai nomor tunggal bernilai 1 hingga 5, dimana 1 merupakan kualitas terburuk dan 5 merupakan kualitas terbaik.

Persepsi pengguna yang direpresentasikan dalam nilai dari MOS ditunjukkan pada tabel dibawah ini.

Tabel 2.2 *Mean Opinion Score* [6]

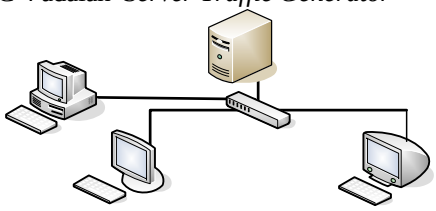
Opini Pengguna	MOS *Score*
Sangat memuaskan	4.3-5.0
Memuaskan	4.0-4.3
Baik	3.6-4.0
Banyak yang tidak puas	3.1-3.6
Buruk	2.6-3.1
Tidak direkomendasikan	1.0-2.6

3. Perencanaan dan Implementasi

3.1 Topologi Jaringan

Topologi yang digunakan dalam pembuatan sistem tersebut dapat dilihat pada gambar 3.1. Pada gambar tersebut ditentukan bahwa sistem menggunakan 3 buah *Personal Computer* (PC), dengan perincian:

- PC 1 adalah *Server VoIP*
- PC 2 adalah *Client 1*
- PC 3 adalah *Client 2*
- PC 4 adalah *Server Traffic Generator*



Gambar 3. 1 Topologi Jaringan VoIP

3.2 Kebutuhan Pendukung Infrastruktur

Kebutuhan akan infrastruktur terbagi menjadi dua macam, yaitu *software* dan *hardware*, dimana keduanya saling mendukung satu sama lain.

1. Server Asterisk
   Dalam tugas akhir ini menggunakan paket asterisk berupa asterisk-trunk revision 61760 yang di download dengan subversion untuk mendowload semua source codenya.
2. LibSRTP
   Dibutuhkan library SRTP untuk menyediakan mekanisme keamanan dengan protokol SRTP. libSRTP ini menggunakan versi SRTP-1.2.4.
3. LibMikey
   Penggunaan asterisk dengan libSRTP perlu adanya *depedencies* paket dengan menggunakan libmikey yang sekaligus dapat digunakan untuk UA (*user agent*) dengan minisip.
4. patch asterisk-srtp-mikey
   patch ini mengandung *script* yang digunakan untuk penggunaan protokol SRTP pada server Asterisk.
5. Snom 360
   Sebagai user agent, snom 360 mempunyai fitur yang dapat mendukung penggunaan protokol SRTP pada jaringan VoIP. Snom 360 dapat di download secara gratis.

3.3 Codec

Pada Tugas Akhir ini digunakan *codec* GSM dan G.711, dengan alasan *codec* ini memiliki rating MOS (*Mean Opinion Score*) terbesar dibandingkan dengan *codec* lainnya. Ini disebabkan karena G.711 menggunakan kompresi yang tidak efesien, sehingga lebih *robust* terhadap *packet loss*. Sedangkan GSM *codec open source* dengan jitter dan throughput yang lebih kecil, yang digunakan sebagai standar selular.

3.4 *Server Traffic Generator*

Iperf merupakan software *traffic* generator yang digunakan untuk memberikan beban *traffic* terhadap jaringan dan dapat didownload di www.dast.nlanr.net. Iperf dapat bekerja di platform windows XP dan software ini hanya dapat dijalankan di command prompt dengan mengeksekusi file .exe dengan mekanisme *client-server*.
Beban yang diberikan sebesar 3 MB dan 5 MB kepada *client* 1 700@10.126.13.200

3.5 Metode Pengamatan Data

Adapun data-data yang diambil saat ujicoba untuk pengambilan data parameter QoS meliputi beberapa konfigurasi jaringan VoIP yaitu :

1. Konfigurasi dengan protokol RTP tanpa beban
   - Menggunakan *Codec* G.711
   - Menggunakan *Codec* GSM
2. Konfigurasi dengan protokol RTP dengan beban 3 MB
   - Menggunakan *Codec* G.711
   - Menggunakan *Codec* GSM
3. Konfigurasi dengan protokol RTP dengan beban 5 MB
   - Menggunakan *Codec* G.711
   - Menggunakan *Codec* GSM
4. Konfigurasi dengan protokol SRTP tanpa beban
   - Menggunakan *Codec* G.711
   - Menggunakan *Codec* GSM
5. Konfigurasi dengan protokol SRTP dengan beban 3 MB
   - Menggunakan *Codec* G.711
   - Menggunakan *Codec* GSM
6. Konfigurasi dengan protokol SRTP dengan beban 5 MB
   - Menggunakan *Codec* G.711
   - Menggunakan *Codec* GSM

4. Data dan Analisa

4.1 *Sniffing* Terhadap Jaringan VoIP

1. Unsecure
   Komunikasi yang berlangsung dalam jaringan ini dengan sangat mudah di sadap oleh *attacker* dengan bukti suara yang disadap dapat di-*capture* dan didengar.
   Penganalisaan dapat dilakukan dengan mengamati protokol SDP (*Session Description Protocol*). SDP yang dikirim dapat di lihat di *debug server* yang dikonfigurasikan di *server* Asterisk CLI dengan perintah

```
.............
m=audio 54754 RTP/AVP 0 101
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
..............
```

2. Secure
   Komunikasi yang berlangsung dalam jaringan ini dengan tidak dapat di sadap oleh *attacker* dengan bukti suara yang disadap tidak dapat didengar.
   Penganalisaan dapat dilakukan dengan mengamati protokol SDP (*Session Description Protocol*). SDP yang dikirim dapat di lihat di *debug server* yang dikonfigurasikan di *server* Asterisk CLI dengan perintah

```
...............
m=audio 58698 RTP/AVP 3 101
a=crypto:1 AES_CM_128_HMAC_SHA1_32
inline:uyIlNHZe1HRih4HRo7qbZIRJys6
rbi1+KjwRPMWR
a=rtpmap:3 gsm/8000
a=rtpmap:101 telephone-event/8000
.....
```

4.2 Pengukuran Parameter QoS

Analisa terhadap parameter QoS VoIP, ada beberapa tahapan yang diambil saat terjadi satu sesi komunikasi yaitu konfigurasi jaringan VoIP tanpa beban

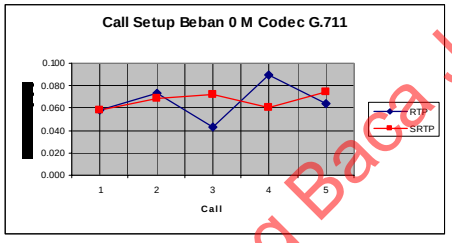
dan pada kondisi jaringan terbebani, beban yang diberikan adalah data dari jaringan internet seperti FTP (*File Transfer Protocol*) untuk pengiriman data, HTTP (*Hypertext Transfer Protocol*) untuk *browsing*, *email* dan lain-lain. Karena pada pengambilan data pada tugas akhir kali ini tidak terhubung ke internet maka penulis menggunakan *Traffic Generator* untuk menggantikan beban tersebut.

Parameter QoS yang diukur meliputi *call setup, end to end delay*, kosumsi *bandwidth, jitter, packet loss* dan MOS. Pengukuran parameter QoS ini dilakukan terhadap jarigan VoIP yang menggunakan protokol RTP dan SRTP yang mana tiap pengukuran jaringan tersebut dibedakan lagi berdasarkan *codec* yang digunakan yaitu G.711 dan GSM.

1. *Call Setup*

Waktu *call setup* adalah waktu yang dilihat dari sisi pemanggil mulai dari dial atau INVITE SDP dalam istilah SIP *message* sampai terminal VoIP yang dipanggil berdering atau dalam istilah SIP *message* 180 *ringging*, misal gambar 4.4 yaitu 0.064 - 0.000 = 0.064 s

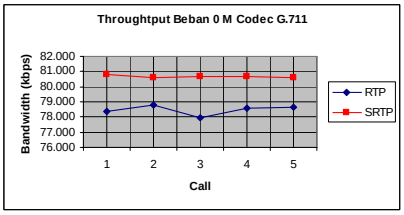
Pada saat konfigurasi jaringan VoIP menggunakan media transfer RTP, nilai call setup rata-rata dengan *codec* G.711, saat tanpa beban adalah 0.065 s dan pada saat konfigurasi jaringan VoIP menggunakan media transfer SRTP adalah 0.067 s, hal ini menunjukkan bahwa dengan penggunaan protokol SRTP pada jaringan VoIP bisa dikatakan sama waktu panggil karena dapat dilihat *range call setup* RTP dan SRTP berada pada nilai 0.043 - 0.058 s. Nilai *call setup* yang terukur dapat dilihat pada gambar 4.5 berikut ini:



Gambar 4. 1 *Call Setup* Beban 0 M *Codec* G.711

2. Konsumsi *Bandwidth*(*Throughput*)

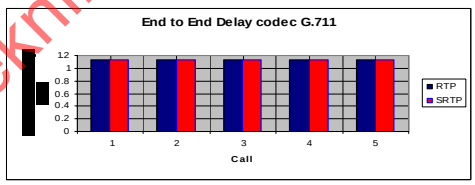
Pada saat konfigurasi jaringan VoIP menggunakan media transfer RTP, nilai kosumsi *bandwidth* rata-rata dengan *codec* G.711, saat tanpa beban adalah 78.467 kbps dan pada saat konfigurasi jaringan VoIP menggunakan media transfer SRTP adalah 80.667 kbps, hal ini menunjukkan bahwa dengan penggunaan protokol SRTP pada jaringan VoIP mengalami kenaikan konsumsi *bandwidth* rata-rata sekitar 2.199 kbps. Meskipun diberi protokol SRTP, suara yang didengar tetap jelas dan tidak putus-putus. nilai konsumsi *bandwidth* yang diperoleh ditunjukkan oleh gambar 4.6 dimana dapat dilihat nilai konsumsi *bandwidth* pada jaringan VoIP dengan RTP lebih rendah dibandingkan dengan SRTP.



Gambar 4. 2 *Throughtput* Beban 0 M *Codec* G.711

3. *End to End Delay*

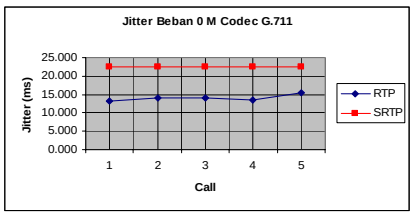
Pada saat konfigurasi jaringan VoIP menggunakan media transfer RTP, nilai *delay end to end* rata-rata dengan *codec* G.711, saat tanpa beban adalah 1.125 ms dan pada saat konfigurasi jaringan VoIP menggunakan media transfer SRTP adalah 1.125 ms. Pengukuran nilai ini tidak dapat dilakukan untuk menunjukkan nilai detil karena aplikasi Wireshark yang digunakan sebagai pengukur parameter QoS tidak dapat mengukur *network delay* dibawah 1 ms. Dari hasil dan gambar 4.7 *network delay* diasumsikan memiliki nilai < 1 ms, sehingga kualitas suara yang diperoleh adalah memuaskan.



Gambar 4. 3 *End to End Delay* Beban 0 M *Codec* G.711

4. *Jitter*

Pada saat konfigurasi jaringan VoIP menggunakan media transfer RTP, nilai *jitter* rata-rata dengan *codec* G.711, saat tanpa beban adalah 14.052 ms dan pada saat konfigurasi jaringan VoIP menggunakan media transfer SRTP adalah 22.491 ms, hal ini menunjukkan bahwa dengan penggunaan protokol SRTP pada jaringan VoIP mengalami kenaikan nilai *jitter* rata-rata sekitar 8.438 ms, hal ini menunjukkan bahwa dengan adanya penggunaan protokol SRTP, maka nilai *jitter* akan bertambah besar. Besarnya nilai *jitter* sangat dipengaruhi besarnya tumbukan antar paket dalam jaringan. Penggunaan protokol SRTP pada jaringan akan menyebabkan semakin besar peluang terjadinya *congestion* dengan demikian *jitter* akan semakin besar. Berdasarkan nilai *jitter* kualitas suara yang peroleh dengan RTP adalah memuaskan, karena nilainya berada antara 0-20 ms dan dengan SRTP adalah dapat diterima karena nilainya berada antara 20 – 50 ms. Nilai *jitter* yang terukur dapat dilihat pada gambar 4.8 berikut ini:



Gambar 4. 4 *Jitter* Beban 0 M *Codec* G.711

5. *Packet Loss*

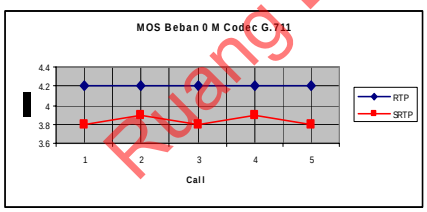
Packet loss untuk konfigurasi jaringan VoIP ini dapat dilihat pada tabel 4.1 dibawah ini. Penyebab utama dari hilangnya paket RTP ini adalah *end to end delay* serta kongesti yang terlalu besar dalam jaringan, pada pengukuran diperoleh *packet loss* 0.00% baik pada saat pengunaan protokol RTP maupun penggunaan protokol SRTP, hal ini dikarenakan *end to end delay* dan *jitter* yang dihasilkan kecil. Berdasarkan nilai *packet loss* kualitas suara yang peroleh adalah memuaskan, karena nilainya adalah 0.00 %.

Tabel 4.1 *Packet Loss* Beban 0 M *Codec* G.711

No	Source	Destination	Packets Loss (%)	
			RTP	SRTP
1	10.126.13.200	10.126.13.201	0.00	0.00
2	10.126.13.200	10.126.13.201	0.00	0.00
3	10.126.13.200	10.126.13.201	0.00	0.00
4	10.126.13.200	10.126.13.201	0.00	0.00
5	10.126.13.200	10.126.13.201	0.00	0.00
Average			**0.000**	**0.000**

6. MOS

Dari gambar 4.9 dapat diketahui bahwa nilai MOS rata-rata yang diperoleh pada saat penggunaan protokol RTP pada konfigurasi jaringan VoIP adalah 4.2 dengan kualitas suaranya adalah memuaskan dan penggunaan protokol SRTP adalah 3.84 dengan kualitas suara baik.



Gambar 4. 5 MOS Beban 0 M *Codec* G.711

5. Kesimpulan

Beberapa hal yang dapat diambil kesimpulan dari Tugas Akhir ini terkait dengan analisa hasil implementasi protokol SRTP dan pengukuran parameter QoS antara penggunaan protokol RTP dan SRTP pada jaringan VoIP adalah sebagai berikut:

1. Dengan melakukan implementasi keamanan jaringan VoIP terhadap transfer media *signalling* RTP dengan menggunakan protokol *Secure* RTP (SRTP) membuat penyadapan suara terhadap hasil *capturing* paket RTP tidak dapat terdengar.
2. Jaringan VoIP yang menggunakan protokol SRTP dapat di implementasikan dengan *proxy/provider* yang mendukung fitur SRTP dan *user agent/softphone* yang mendukung SRTP.
3. Penerapan teknologi SRTP sebagai sistem keamanan data pada jaringan VoIP tidak terlalu mempengaruhi kualitas suara berdasarkan MOS yang didapat.
4. Pengunaan jenis codec sebagai *voice coding* mempengaruhi *end to end delay*, *jitter* dan *throughput* jaringan VoIP.
5. Pada saat kondisi jaringan VoIP terbebani kenaikan nilai parameter QoS tidak terlalu signifikan baik jaringan VoIP dengan dengan RTP maupun SRTP.

6. DAFTAR PUSTAKA

[1] Ahmar Ghaffar, **Security in VoIP Environment** http://www.snom.com/wiki/index.php/Security_in_VoIP_environments,Juni 2003

[2] Andreas Steffen, Daniel Kaufmann, Andreas Stricke, **SIP Security**, security group,CH-8401 Winterthur,2003

[3] …., **SER, SIP Express Router**, http://iptel.org/ser, Mei 2007.

[4] Dr. Peter J. Welcher, **Quality of Service for Voice Over IP**, Presentation for Chesapeake Netcraftsmen, Chesapeake Netcraftsmen , 2003.

[5] …., **Performance Analysis for VoIP System**, http://w.csie.org/~acpang/course/voip_2005_fall/presentation/B2. ppt, Juni 2007.

[6] Onno W. Purbo, **VoIP Cikal Bakal "Telkom Rakyat",** Info Komputer, Jakarta, 2007

7. RIWAYAT HIDUP PENULIS

Fauzar Amin. Dilahirkan di Pekanbaru, pada tanggal 19 Agustus 1983. merupakan anak ke tiga dari empat bersaudara dari pasangan Armiyn dan Fauziah. Penulis menyelesaikan pendidikan sekolah dasar di SDN 001 Pekanbaru kemudian menamatkan sekolah menengah pertama di SLTPN 2 Pekanbaru. Kemudian penulis melanjutkan ke SMUN 2 Pekanbaru tamat pada tahun 2001. Penulis menyelesaikan pendidikan Diploma-III di Politeknik Caltex Riau dengan jurusan Teknik Komputer pada Januari 2005. Kemudian melanjutkan ke Program Lintas Jalur Institut Teknologi Sepuluh November di jurusan Teknik Informatika FTIF-ITS pada bulan Agustus 2005.

E-mail : fauzaramin@yahoo.com
Phone : +62 813 7129 3723