Analisa Kinerja VoIP Client dengan Menggunakan Modul RTP Terenkripsi dan SRTP pada Jaringan VoIP

Hendra Prastiawan

Cargill Indonesia, Wisma 46 Kota BNI
hendra.prastiawan2@gmail.com

Abstrak

Seiring dengan berkembangnya teknologi telekomunikasi dan komputer, banyak aplikasi-aplikasi yang mendukung komunikasi telepon melalui jaringan internet tumbuh dan berkembang. Layanan yang dimaksud adalah Voice over Internet Protocol atau biasa disebut dengan VoIP. VoIP yang menggunakan server-server gratis yang ada saat ini tidaklah menjamin keamanan dari sebuah percakapan yang dilakukan didalamnya. Oleh sebab itu, diperlukan sebuah VoIP Client yang dapat mengamankan data komunikasi tersebut. Walaupun sekarang sudah tersedia sebuah protokol aman dalam VoIP yang disebut SRTP atau Secure Real-Time Protocol, namun hal tersebut perlu dilakukan pengujian lebih lanjut dari kualitas layanan dengan membandingkan protokol tersebut dengan sebuah protokol biasa yang ditambahkan sebuah algoritma enkripsi untuk mengetahui kinerja protokol yang lebih baik digunakan dalam VoIP tersebut. Algoritma yang akan ditambahkan dalam protocol tersebut yaitu algoritma AES (Advanced Encryption Standard).

Kata Kunci: VoIP, Enkripsi, Kualitas Layanan

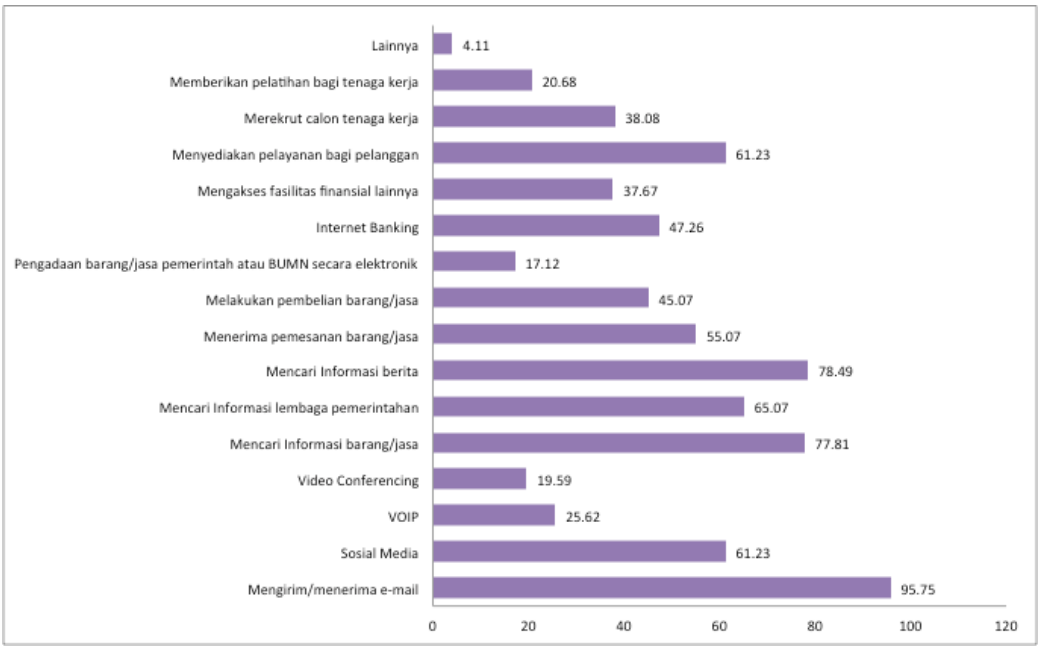
Abstract

Along with the development of telecommunications technology and computer, there are many applications that support telephone communication using internet connection. This service is called Voice Over Internet Procotol, which is VoIP in short. VoIP using free servers does not guarantee the conversation security. Therefore, it is required a VoIP Client that is able to secure the communication data. Although recently a secure protocol in VoIP which is called SRTP or Secure Real-Time Protocol is already available, a further test should be done of service quality by comparing the protocol to an encrypted-algorithm reguler protocol to know which protocol that has better performance to be used in the VoIP. The algorithm which is included in the protocol is AES (Advanced Encrytption Standard) algorithm.

Keywords : VoIP, Encryption, Quality of Service

1. PENDAHULUAN

Pemanfaatan Teknologi Informasi dan Komunikasi (TIK) di Indonesia saat ini sangat pesat. Hal ini tercermin dari berkembangnya pengguna internet yang tentunya berpengaruh pada kegiatan yang dilakukan oleh pengguna internet. Asosiasi Penyelenggara Jasa Internet (APJII) bekerjasama dengan Badan Pusat Statistik (BPS) melakukan survei mengenai pengguna internet di Indonesia pada tahun 2013. Berikut adalah hasil survei yang dilakukan oleh APJII dan BPS tersebut (Gambar 1)



Gambar 1 Persentase pengguna internet berdasarkan aktivitasnya di internet (Sumber: Hasil Survei Penggunaan dan Penyerapan Sarana Komunikasi dan Teknologi Informasi (P2SKTI) 2013 – APJII-BPS)

Dari hasil survei diatas dapat dilihat bahwa aktivitas yang paling sering dilakukan oleh pengguna internet di Indonesia yaitu mengirim dan menerima e-mail yaitu sebesar 95.75%, mengalami penurunan sebesar 1.94% bila dibandingkan pada tahun 2011 yang mempunyai presentase 97.69%. Sedangkan aktivitas paling rendahnya yaitu lainnya seperti promosi hotel sebesar 4.11%, Setelah itu menyusul aktivitas pengadaan barang secara elektronik sebesar 17.12%, Video Conferencing sebesar 19.59%, dan VOIP sebesar 25.62%.

Voice over Internet Protocol (VoIP) adalah teknologi yang memungkinkan percakapan suara jarak jauh melalui media internet. Data suara diubah menjadi kode digital dan dialirkan melalui jaringan yang mengirimkan paket-paket data, dan bukan melalui sirkuit analog seperti halnya telepon biasa. Dalam komunikasi VoIP, pemakai melakukan hubungan telepon melalui terminal yang berupa PC atau telepon biasa. Dengan bertelepon menggunakan VoIP, banyak keuntungan yang dapat diambil diantaranya adalah dari segi biaya jelas lebih murah dari tarif telepon tradisional,

karena jaringan IP bersifat global. Kemudian penggunaan bandwidth yang lebih kecil daripada telepon biasa. Dengan majunya teknologi penggunaan bandwidth untuk voice sekarang ini menjadi sangat kecil. Teknik pemanfaatan data memungkinkan suara hanya membutuhkan sekitar 8kbps bandwidth.

Selain memiliki keuntungan dari segi biaya, VoIP juga memiliki kelemahan, Kelemahan dari VoIP yaitu kualitas suara tidak sejernih jaringan PSTN atau telepon konvensional. Hal ini disebabkan efek dari kompresi suara dengan bandwidth kecil maka akan ada penurunan kualitas suara dibandingkan jaringan PSTN konvensional.

Permasalahan yang sering terjadi dalam VoIP yaitu mengenai masalah keamanan data dari percakapan yang terjadi serta kinerja didalam VoIP tersebut. Penyedia jasa VoIP gratis seperti Skype, WhatsApp, Line, voiprakyat.org, dan lain-lain tidak menjamin keamanan data komunikasi tersebut. Walaupun dengan berkembangnya teknologi, hadirlah protokol jaringan yang aman seperti Secure Real-Time Protocol perlu diuji kembali dengan membandingkan dengan protokol jaringan yang sudah ditambahkan metode enkripsi tertentu, salah satunya dengan metode AES atau Advanced Encryption Standard. Untuk itu, maka dalam penelitian ini akan dilakukan pengujian antara dua protokol jaringan tersebut agar mengetahui kinerja dari VoIP Client tersebut yang dihasilkan dari keduanya.

Perumusan masalah yang akan ditentukan dalam penelitian ini adalah sebagai berikut:

1. Bagaimana mengintegrasikan VoIP client Peers dengan menambahkan modul enkripsi AES dan SRTP?
2. Bagaimana mengukur kinerja dari VoIP client Peers yang sudah diamankan?
3. Bagaimana hasil kuesioner di sisi pengguna dari penggunaan VoIP Client Peers yang diintegrasikan dengan modul enkripsi AES dan SRTP?

Tujuan dari penelitian ini yaitu untuk mengetahui jaringan protokol dengan performa yang lebih baik antara secure real-time protocol dan Real-time Transport Protocol yang sudah ditambahkan fitur enkripsi dengan algoritma *Advanced Encryption Standard* (AES) dalam komunikasi antara satu client dengan client yang lain. Sedangkan manfaat dari penelitian ini adalah mendapatkan sebuah VoIP client yang memiliki fitur performa yang maksimal ketika melakukan komunikasi antar client.

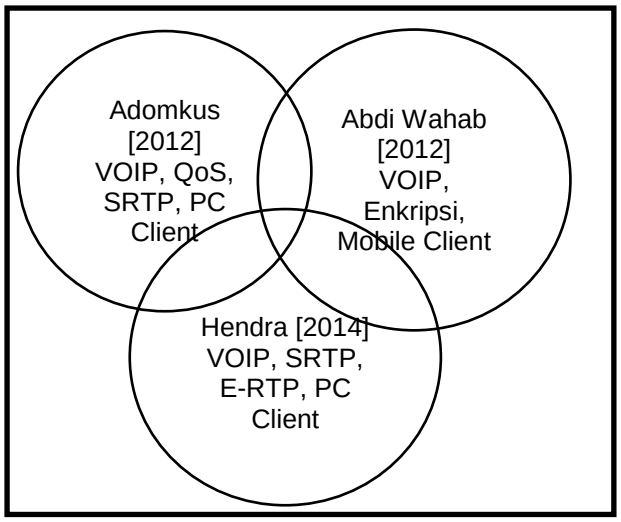
Lingkup penelitian ini atau batasan-batasan pada penelitian ini adalah sebagai berikut:

(1) Aplikasi VoIP client yang digunakan adalah VoIP Peers yang sudah dimasukan metode SRTP dan RTP terenkripsi.
(2) Metode enskripsi yang digunakan dalam RTP adalah *Advanced Encryption Standard*.

(3) Data yang diambil berasal dari pengukuran dan pengamatan data menggunakan alat pemantau jaringan, seperti Wireshark.
(4) Jaringan yang digunakan menggunakan *wireless* LAN.
(5) Penelitian ini dibatasi hanya mengukur kinerja dari VoIP Peers yang sudah dimasukan metode SRTP dan RTP Terenkripsi.
(6) Bahasa pemrograman yang digunakan adalah Bahasa Pemrograman Java.
(7) *Tools* pemrograman yang digunakan yaitu Netbeans.

2. PENELITIAN TERKAIT

Adapun beberapa penelitian lama yang terkait dengan penelitian ini yaitu antara lain penelitian yang dilakukan oleh Adomkus pada tahun 2008 dengan judul "*Investigation of VoIP Quality of Service using SRTP Protocol*" dan juga penelitian yang dilakukan oleh Abdi Wahab di tahun 2012. Perbedaan dari kedua penelitian tersebut dengan penelitian ini dapat dilihat pada Gambar 2 dibawah ini.



Gambar 2 Penggambaran Penelitian Terkait dengan Penelitian Ini

Pada penelitian pertama, Adomkus melakukan penelitian VOIP yang lebih memfokuskan pada kualitas layanan untuk *media session* yang aman. VOIP memiliki karakteristik yang sangat khusus yang disebut *Time Critical* karena waktu memiliki dampak yang memperngaruhi kualitas layanan, dan dan dalam mengirimkan sebuah informasi. Jadi, Adomkus melakukan percobaan pada VOIP untuk memastikan aliran data dan komunikasi aman dan memberikan kualitas yang maksimal.

Pemodelan VOIP yang digunakan oleh Adomkus untuk memastikan panggilan aman yaitu dengan menggunakan Opnet Modeler. Hasil dari penelitian Adomkus ini memperlihatkan bahwa dalam hal apapun *delay* dari paket suara yang tidak melebihi *time critical* sebesar 150 ms dan kita dapat memastikan kualitas layanan untuk mengenkripsi paket suara pada jaringan VOIP.

Sedangkan penelitian lain yang berhubungan dengan penelitian ini adalah penelitian yang dilakukan oleh Abdi Wahab di tahun 2012 yang berjudul "Analisis Kinerja VOIP Client Sipdroid dengan Modul Enkripsi Terintegrasi". Abdi Wahab membuat sebuah percobaan untuk mengetahui kinerja dari VOIP dengan menambahkan sebuah modul enkripsi didalam layanan VOIP tersebut. Adapun metode enkripsi yang diintegrasikan yaitu AES, DES, dan RC4. Percobaan dari modul enkripsi ini dilakukan pada perangkat telepon seluler yang mempunyai sistem operasi Android. Hasil dari penelitian ini yaitu Sipdroid dengan modul enkripsi menurut analisa penulis mampu mengatasi dari penyerangan pasif yang bersifat mendengarkan informasi (eavesdropping) pada komunikasi VoIP yang dilakukan. Dengan demikian, penelitian ini menjadi salah satu rujukan pada penelitian ini.

2.1. AES (*Advanced Encryption Standard*)

Advanced Encryption Standard adalah (AES) adalah skema enkripsi menggantikan 3DES yang dinilai sudah tidak memenuhi lagi dengan alasan efisiensi dan keamanan. AES memiliki kekuatan keamanan yang sama dengan 3DES, tetapi memiliki efisiensi yang lebih baik dibandingkan 3DES. Untuk itu, NIST menentukan bahwa AES menggunakan *symmetric block cipher* dengan panjang block 128 bit dan mendukung panjang kunci mulai dari 128 bit, 192 bit, dan 256 bit.

Input dan output dari algoritma AES terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi ciphertext. Cipher key dari AES terdiri dari key dengan panjang 128 bit, 192 bit, atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah round yang akan diimplementasikan pada algoritma AES ini.

2.2. SRTP (Secure Real-Time Protocol)

Secure Real Time Protocol adalah sebuah profile dari Real-time Transport Protocol yang menyediakan layanan kerahasiaan, otentikasi pesan, dan reply protection terhadap paket RTP dan RTCP. SRTP melindungi lalu lintas suara pada lapisan aplikasi. SRTP akan mengenkripsi payload multimedia (suara).

Untuk enkripsi dan dekripsi dari aliran data, SRTP menggunakan AES (Advance Encryption Standart) sebagai cipher default. Ada dua mode yang didefinisikan oleh cipher AES untuk digunakan sebagai stream cipher yaitu AES-CM (Advance Encryption Standart – Counter Mode) dan AES F8. SRTP membutuhkan dua buah jenis kunci yaitu master key dan session key. Session key artinya kunci yang secara langsung digunakan dalam cryptographic transform.

Untuk mengotentikasi pesan dan melindungi integritas, digunakan algoritma HMAC-SHA1. HMAC dihitung atas payload dan bahan dari header paket, termasuk

nomor urut paket. Untuk melindungi terhadap serangan replay, penerima mempertahankan indeks pesan yang sebelumnya diterima, membandingkan indeks pesan dengan indeks dari setiap pesan yang diterima baru dan mengakui pesan baru hanya jika belum dikirim sebelumnya.

Pada prinsipnya, SRTP mempunyai sistem kerja yang sama dengan RTP yaitu mendukung dan mengusahakan agar komunikasi VoIP dapat berlangsung secara real-time. Hanya saja pada format protokol SRTP diberikan penambahan SRTP message yang berguna untuk memberikan fasilitas enkripsi.

Sebelum terjadi pengiriman komunikasi VoIP, akan dilakukan pertukaran kunci master antara dua client yang saling berkomunikasi. Kunci master ini dapat digenerate menjadi dua kunci sesi, yaitu kunci sesi enkip dan kunci sesi autentikasi. Kunci enkrip digunakan untuk untuk mengenkripsi data VoIP sehingga terhindar dari hal yang sifatnya pencurian maupun perusakan informasi. Sedangkan kunci autentikasi digunakan sebagai validasi data dan memastikan bahwa penerima adalah tujuan yang benar untuk mencegah hal yang sifatnya pemalsuan identitas.

Setelah terjadi pertukaran kunci, maka kunci-kunci tersebut akan digunakan untuk mengenkrip data sebelum data tersebut dikirimkan. Kunci sesi ini akan berubah-ubah pada suatu waktu tertentu secara *random*.

2.3. Kualitas Layanan

Kualitas layanan atau biasa disebut dengan *Quality of Service* adalah sebuah parameter yang sering digunakan untuk mengukur performa jaringan. Jadi, QoS dengan kata lain digunakan untuk mengevaluasi lingkungan jaringan dimana VOIP akan dijalankan. Berikut adalah parameter QoS jaringan, antara lain:

Tabel 1 Parameter QoS Jaringan

Kategori	**Parameter**
Timeliness	*Delay*
	Jitter
	Response time
Bandwidth	*System-level data rate*
	Application-level data rate
	Transaction time
Reliability	*Mean time to failure* (MTTF)
	Mean time to repair (MTTR)
	Mean time between failures (MTBF)
	Percentage of time available
	Packet loss rate
	Bit error rate

Berikut ini akan dijabarkan beberapa parameter yang akan digunakan pada penelitian ini.

- Delay
  Delay adalah waktu yang diperlukan sebuah bit data untuk melewati sebuah jaringan dari sebuah node ke node yang lainnya. Terdapat tiga buah delay, yaitu
  - Delay transmisi
  - Delay propagasi
  - Delay pemrosesan

  Performa dinilai baik jika nilai *delay* yang dihasilkan semakin kecil. Untuk menghitung sebuah *delay* dapat dirumuskan sebagai berikut:

  Delay = Waktu Tiba – Waktu kirim

  Atau

  Delay = Waktu selesai proses – Waktu mulai proses

- Packet loss

Packet loss adalah jumlah paket data yang hilang atau tidak terkirim ke tujuan selama terjadinya koneksi. Semakin kecil nilai dari *packet loss*, maka performa yang ditunjukkan akan semakin baik. Berikut adalah rumus untuk menghitung *packet loss*:

Packet Loss = ∑ Paket dikirim - ∑ Paket diterima

- Throughput

Throughput atau yang biasa disebut dengan *bandwidth* adalah rata-rata data (*data rate*) dalam bit per second (bps). *Throughput* biasa disebut dengan kapasitas. Untuk mendapatkan *throughput* yang baik diperlukan *overhead protocol* yang baik. *Overhead protocol* ini memiliki dua buah komponen yaitu *header bits* dan *control overhead*.

2.4. *Mean Opinion Score* (MOS)

Mean opinion score merupakan rekomendasi ITU P.800 yang digunakan untuk mengukur kinerja dari suatu komunikasi multimedia melalui jaringan berdasarkan pandangan dari end user.

Di dalam jaringan komunikasi multimedia (seperti audio, video, atau voice telephony) terutama ketika codec digunakan untuk mengkompresi bandwidth yang dibutuhkan untuk komunikasi tersebut, maka dibutuhkan MOS untuk mengukur sejauh mana kualitas dari komunikasi tersebut berdasarkan perspektif end user. End user akan memberikan penilaian dengan range angka 1 -5 dimana, angka 1 berarti kualitas yang amat buruk dan angka 5 adalah kualitas yang sangat baik.

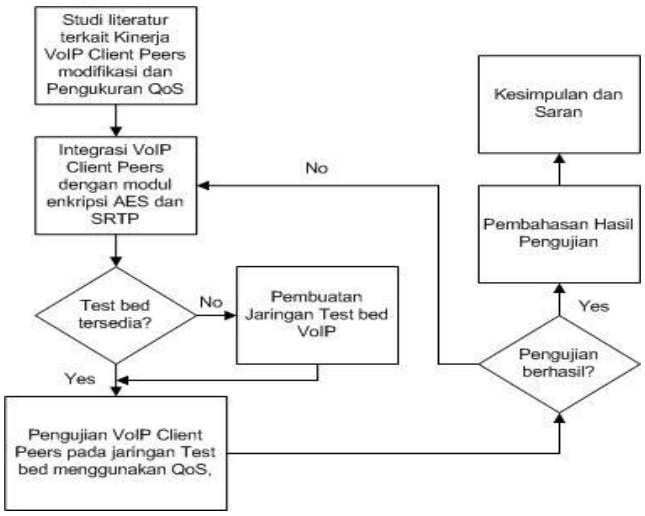
Tabel 2 Nilai MOS yang direkomendasikan ITU-T

Nilai	Kualitas Pembicaraan
5	Excellent
4	Good
3	Fair
2	Poor
1	Bad

3. Metodologi Penelitian

Adapun metodologi yang digunakan pada penelitian ini akan digambarkan pada bagan di Gambar 3.

Sebagaimana terlihat pada bagan di atas bahwa terdapat 6 tahapan yang digunakan didalam penelitian ini mulai dari studi literatur hingga pengambilan kesimpulan dari penelitian ini. Berikut adalah tabel korelasi antara metode, *tool* atau perangkat, parameter dan hasil yang digunakan pada penelitian ini.



Gambar 3 Metodologi Penelitian

Tabel 3 Korelasi antara metode, perangkat, parameter, dan hasil

No.	Metode/Teknik	Perangkat	Parameter	Hasil
1.	Pembuatan skema enkripsi AES dan SRTP	JCE	- Kunci - Data	Modul Enkripsi dengan AES dan SRTP
2.	Integrasi VoIP Client Peers dengan Modul Enkripsi	Modul Enkripsi, Source VoIP Client Peers		VoIP Client RTP Terenkripsi dan VoIP Client SRTP (VoIP Client dengan protokol SRTP)
3	Pembuatan Jaringan *Test bed*	VoIP Client, VoIP Server		Test bed jaringan VoIP
4	Pengukuran kinerja VoIP Client	Wireshark, *Test bed*, jaringan	Delay, packet loss, throughput,	Data pengukuran kinerja VoIP Client

	Peers dengan fitur AES Ter-enkripsi dan SRTP	VoIP, PC Client, survei		

3.1. Perancangan Modul Enkripsi pada VoIP Client Peers

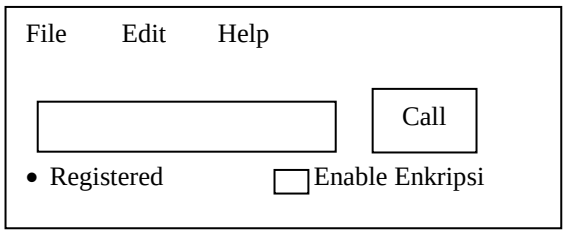
Modul Enkripsi yang digunakan oleh penulis dalam penelitian ini yaitu dengan menambahkan modul enkripsi AES dan sebuah protokol SRTP secara terpisah. Modul AES dan SRTP yang ditambahkan kedalam VoIP Client Peers ini dimaksudkan untuk mengamankan data yang akan dikirimkan pada jaringan VoIP yang telah tersedia dan akan menjadi tambahan fitur baru didalam VoIP Client.

Modul enkripsi tersebut akan bekerja sesuai dengan metode enkripsi yang digunakan. Komunikasi antara dua buah VoIP Client Peers akan berjalan jika metode enkripsi yang digunakan antara dua buah *client* tersebut sama. Namun sebaliknya, jika salah satu *client* menggunakan metode yang berbeda dari *client* satunya, maka komunikasi tidak dapat dilakukan karena data suara yang dikirim dan diterima oleh kedua *client* yang melakukan komunikasi tidak akan dapat di dekripsi balik.

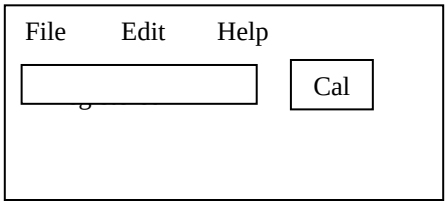
3.2. Perancangan Integrasi Modul Enkripsi pada VoIP Client

VoIP Client Peers yang akan dibuat akan ditambahkan modul enkripsi AES yang sudah diberi tambahan enkripsi sebelumnya dan juga akan ditambahkan protokol SRTP secara terpisah dengan modul enkripsi AES. Modul tersebut akan dibuat dengan menggunakan JCE (*Java Cryptography Extension*).

Adapun rancangan dari Integrasi modul enkripsi AES ini dengan aplikasi VoIP Client Peers akan digambarkan pada gambar dibawah ini:



Gambar 4 Rancangan Antarmuka VoIP Client Peers (AES Ter-enkripsi)

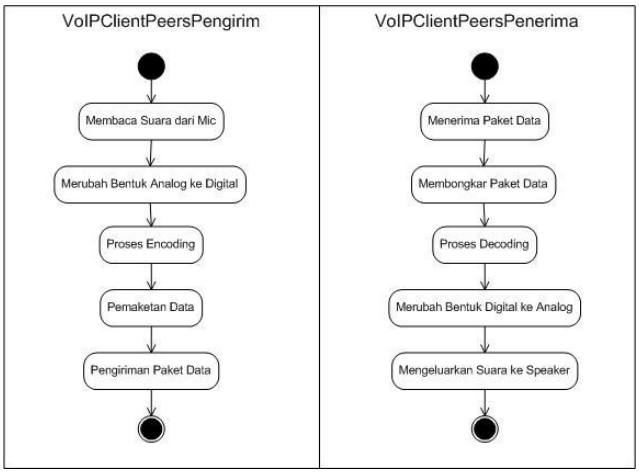


Gambar 5 Rancangan Antarmuka VoIP Client (SRTP)

Akan ada 2 aplikasi VoIP Client Peers yang nantinya akan disimulasikan pada penelitian ini. Yang pertama yaitu VoIP Client Peers yang didalamnya sudah ditambahkan modul enkripsi AES yang sudah ditambahkan enkripsi sebelumnya (Gambar 4), dan aplikasi VoIP Client Peers yang ditambahkan fitur SRTP yang bisa dilihat pada gambar 5.

VoIP Client Peers pada gambar 4 jika pengguna ingin mengaktifkan fitur enkripsinya hanya dengan mencentang fitur "Enable Enkripsi" pada aplikasi tersebut. Sedikit berbeda dengan tampilan VoIP Client SRTP yang tidak ada tambahan fitur "Enable Enkripsi" karena dengan menjalankan aplikasi VoIP Client Peers SRTP ini maka akan otomatis aplikasi dalam keadaan mode aktif untuk fitur penggunaan SRTP tersebut.

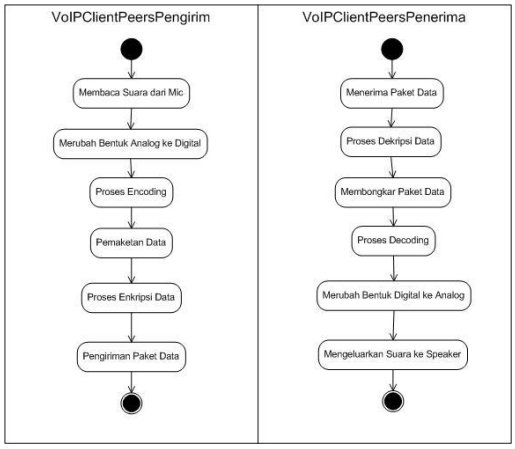
Berikut ini merupakan diagram aktivitas (*activity diagram*) dari VoIP Client Peers sebelum diintegrasikan dengan modul enkripsi AES-Terenkripsi dari JCE.



Gambar 6 *Activity Diagram* VoIP Client Peers

Pada gambar 6 di atas, VoIP Client Peers bekerja seperti sebagaimana VoIP Client yang sudah ada. Mulai dari membaca suara dari microphone, kemudian merubah suara analog ke digital. Setelah proses perubahan suara dari analog ke digital maka proses selanjutnya yaitu meng-*encoding* lalu hasilnya kemudian dibuat paket data hingga paket data tersebut dikirim ke VoIP Client Peers tujuan. Begitu juga terjadi pada VoIP Client Peers tujuan, dimulai dari menerima paket data yang dikirim kemudian paket data tersebut dibongkar dan masuk proses *decoding* dan merubah digital ke analog dan terakhir mengeluarkan suara ke speaker.

Sedangkan *activity* diagram untuk VoIP Client Peers yang sudah dimodifikasi adalah sebagai berikut:



Gambar 7 *Activity Diagram* VoIP Client Peers Modifikasi

Adapun perbedaan antara VoIP Client yang biasa digunakan dengan VoIP Client yang sudah ditambahkan modul enkripsi yaitu pada VoIP Client yang sudah dimodifikasi, sebelum data dikirimkan, terjadi proses enkripsi data terlebih dahulu. Setelah data tersebut di enkripsi, barulah paket data tersebut dikirimkan. Selanjutnya di sisi penerima, terjadi penambahan proses juga. Terjadi proses dekripsi data terlebih dahulu setelah data diterima. Baru selanjutnya proses-proses yang lainnya berjalan sama seperti VoIP Client pada umumnya.

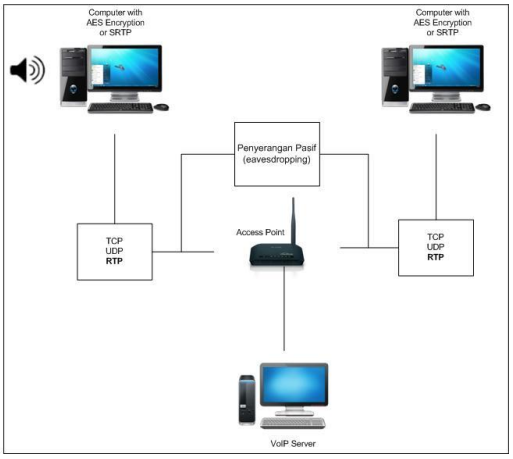
Didalam kode program dari VoIP Client Peers terdapat kode program dimana terdapat metode untuk melakukan enkripsi dan dekripsi dengan menggunakan algoritma AES Terenkripsi dan SRTP. Jad sebelum paket dikirim dalam bentuk RTP, maka data yang ada di dalam RTP *payload* akan diamankan dengan metode-metode yang ada di dalam kode program VoIP Client tersebut.

3.3. Perancangan Test Bed untuk Jaringan VoIP

Adapun perancangan *test bed* untuk jaringan VoIP ini dilakukan sebagai media untuk pengujian modul enkripsi yang telah diintegrasikan dengan VoIP Client Peers. Test bed ini juga sebagai media untuk pengambilan data berdasarkan dari parameter-parameter yang telah ditentukan sebelumnya dalam penelitian ini.

Test bed untuk jaringan VoIP ini digunakan untuk memudahkan dalam pengambilan data sehingga dapat optimal dan meminimalisir rintangan-rintangan ataupun hambatan seperti *bandwidth* yang tidak stabil kemungkinan terjadinya server VoIP yang turun jika menggunakan jaringan VoIP umum.

Berikut skema dari test bed jaringan VoIP yang akan digunakan pada penelitian ini:



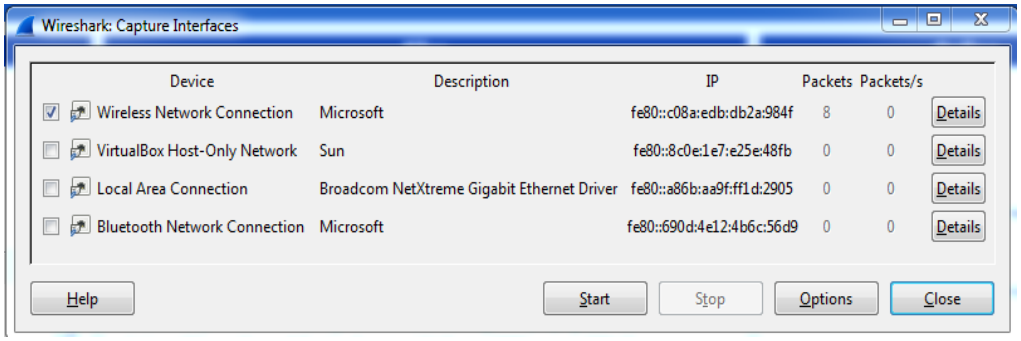
Gambar 8 Test Bed jaringan VoIP untuk VoIP Client Peers

Jaringan test bed yang dibangun untuk VoIP Client Peers ini terdiri dari satu buah server yang sudah terinstall aplikasi server VoIP dan dua buah Client yang sudah terinstall VoIP Client Peers. Sedangkan untuk media transmisinya akan menggunakan *Wireless* LAN.

4. PROSES PENGAMBILAN DATA DARI KOMUNIKASI VoIP

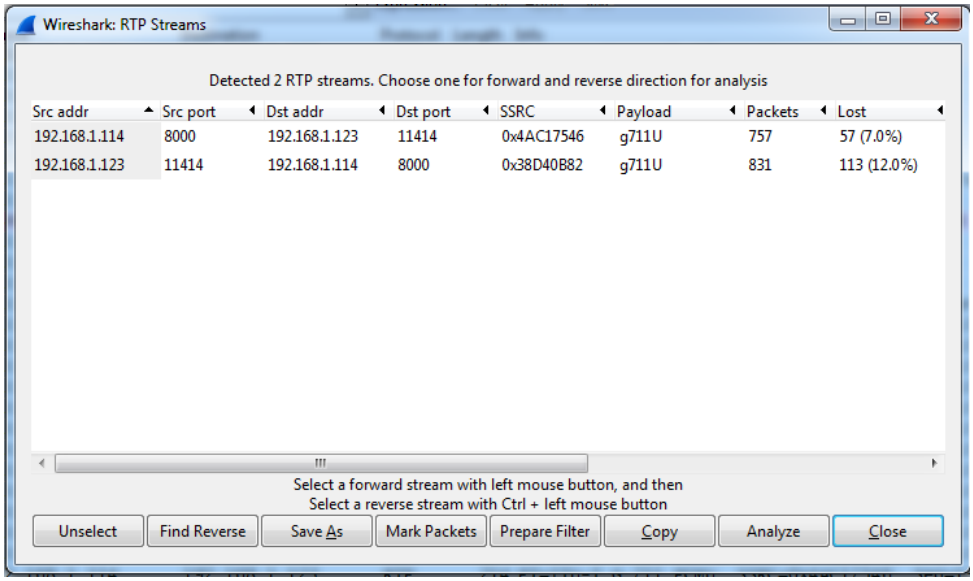
Proses komunikasi pada VoIP yang dilakukan dengan VoIP Client Peers menggunakan paket RTP sebagai pembawa data. Proses pengambilan data dari komunikasi VoIP itu sendiri menggunakan salah satu perangkat (*tool*) yang telah disediakan oleh Wireshark.

Berikut adalah tampilan dari proses penangkapan komunikasi data di VoIP Client Peers pada proses komunikasi VoIP jaringan test bed yang dibangun:



Gambar 9 Proses Penangkapan paket data saat proses komunikasi VoIP Client Peers di Test Bed

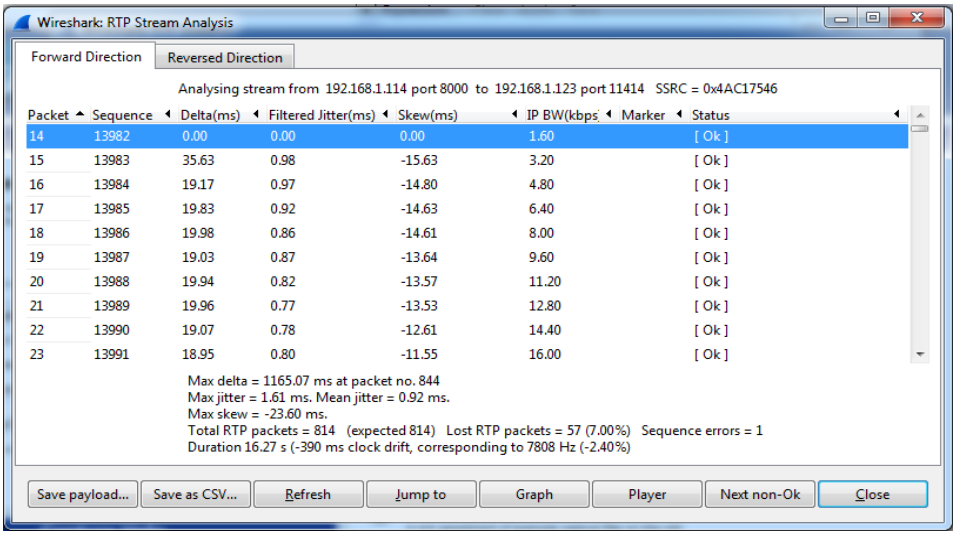
Saat pengguna memulai dengan menekan tombol Start, maka Wireshark akan mulai menangkap semua komunikasi yang sedang terjadi. Dan saat komunikasi VoIP Client Peers tersebut berlangsung, maka Wireshark akan menangkap datanya sebagai berikut:



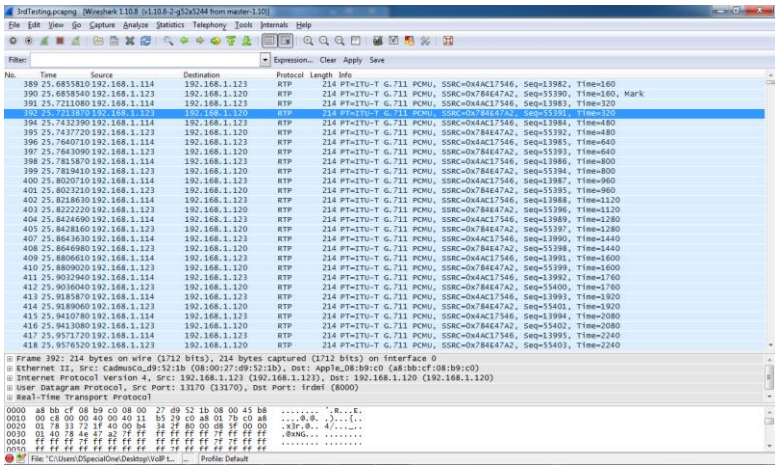
Gambar 10 Hasil paket data yang tertangkap oleh Wireshark saat komunikasi VoIP berlangsung

Selama proses penangkapan data menggunakan Wireshark yang terlihat pada gambar 10, bahwa paket yang tertangkap adalah paket data RTP selama proses komunikasi. Dan terdapat dua buah IP yang melakukan komunikasi tersebut, yaitu IP milik pengguna dan IP dari server VoIP.

Untuk mengambil seluruh data dari paket RTP yang akan dianalisa menggunakan aplikasi pengolah data seperti spreadsheet. Penulis menggunakan salah satu menu didalam Wireshark yaitu menu Telephony yang didalamnya terdapat menu RTP. Kemudian terdapat menu Show All Strems. Akan terbuka jendela baru dengan tampilan sebagai berikut:



Gambar 11 Tampilan RTP Stream yang tertangkap Wireshark



Gambar 12 Hasil analisa RTP stream di Wireshark

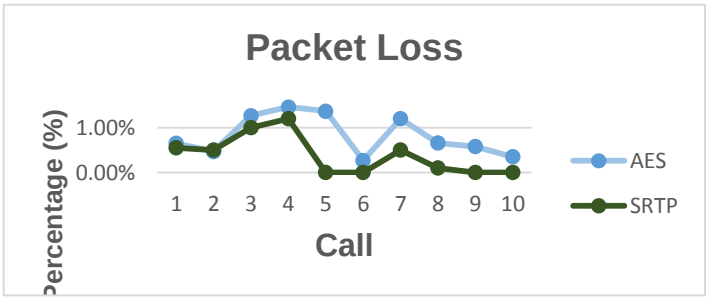
Pada gambar di atas terdapat dua buah RTP stream yang tertangkap oleh Wireshark. Untuk mengambil data yang akan di analisa, hanya perlu mencari pasangan dari RTP stream yang tertangkap. Setelah itu, menekan tombol Analyze. Akan muncul jendela baru sebagai berikut:

Pada jendela di gambar 12, data RTP diambil dengan menyimpan terlebih dahulu ke dalam bentuk CSV (*Comma Separated Value*). Setelah itu data diolah dengan menggunakan aplikasi spreadsheet untuk menghitung parameter-parameter yang akan dicari pada penelitian ini, yaitu *Delay*, *Packet Loss*, dan *Throughput*.

4.1. Pengujian Kualitas Layanan (*Quality of Service* (QoS))

Adapun pengujian dari kualitas layanan pada penelitian ini meliputi 3 parameter yang telah ditentukan, antara lain *Delay*, *Packet Loss*, dan *Throughput*.

VoIP client Peers akan diukur performanya berdasarkan *packet loss* yang terjadi selama komunikasi VoIP berlangsung. Adapun hasil yang didapat setelah 10 kali pengujian di jaringan test bed dapat dilihat dari gambar di bawah ini.

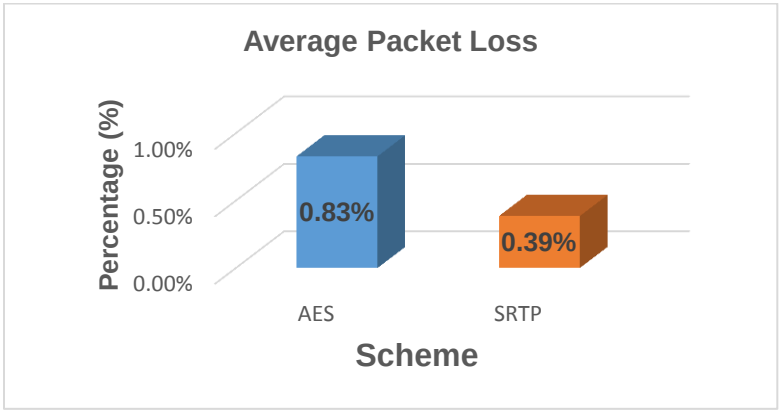


Gambar 13 Hasil pengukuran *Packet Loss*

Hasil pengukuran di atas menunjukkan bahwa VoIP Client Peers dengan skema SRTP memiliki *packet loss* terendah, sedangkan VoIP Client Peers dengan

menggunakan skema modul enkripsi AES memiliki *packet loss* lebih besar bila dibandingkan dengan skema SRTP.

Selanjutnya akan ditampilkan diagram dari rata-rata *packet loss* hasil dari pengujian. Diagram tersebut terlihat dari gambar dibawah ini:



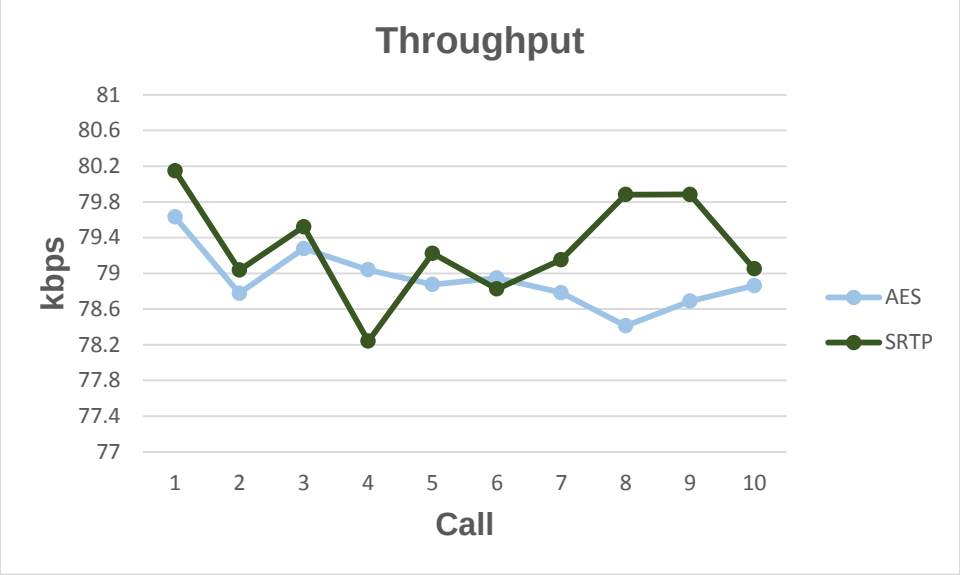
Gambar 14 Rata-rata *Packet Loss*

Hasil gambar 14 diatas menggambarkan bahwa VoIP Client Peers dengan menggunakan skema SRTP memiliki rata-rata *packet loss* paling kecil dibandingkan dengan VoIP Client Peers yang diintegrasikan dengan modul enkripsi AES. Sedangkan VoIP Client Peers yang diintegrasikan dengan modul enkripsi memiliki rata-rata *packet loss* lebih besar dari SRTP.

Performa yang ditunjukkan dari *packet loss* berhubungan dengan komunikasi yang sering terputus atau tidaknya dalam sebuah sesi komunikasi VoIP. Hasil yang didapatkan di atas menunjukkan bahwa VoIP Client Peers dengan skema SRTP menjadi yang terbaik diantara VoIP Client Peers yang diintegrasikan dengan modul enkripsi AES.

4.2. Hasil Pengujian Throughput

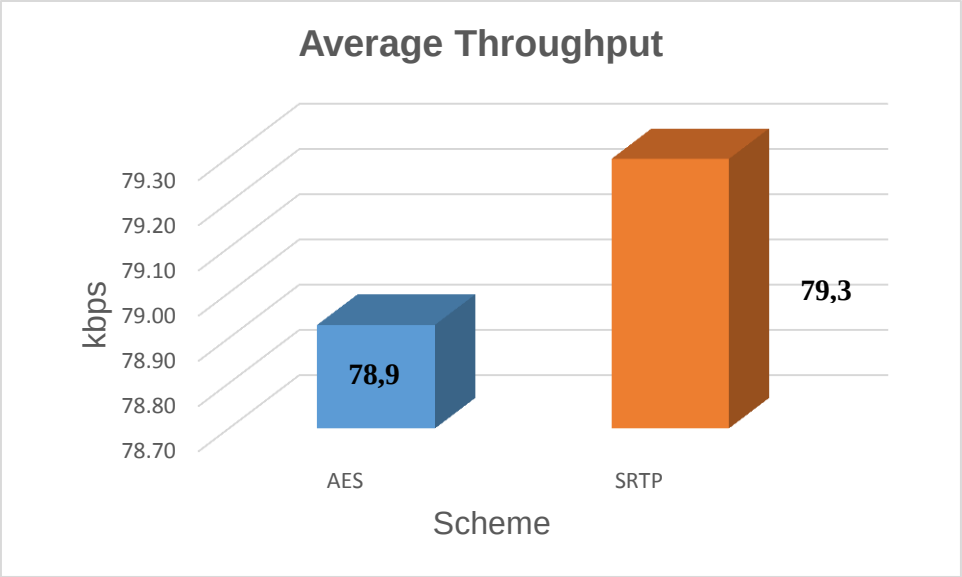
Untuk pengukuran selanjutnya yang digunakan di dalam penelitian ini yaitu pengukuran dengan menggunakan parameter throughput. Throughput yang didapatkan dari pengukuran pada jaringan test bed yang dibangun adalah sebagai berikut:



Gambar 15 Hasil Pengukuran *Throughput*

Throughput yang dihasilkan oleh kedua skema di atas berkisar dari 78.24 kbps hingga 80.14 kbps. Hal ini termasuk dari rata-rata *throughput* dari VoIP yang tertera di http://www.voip-info.org/wiki/view/Bandwidth+consumption yaitu berkisar antara 64 kbps hingga 87.2 kbps. Pada setiap skema VoIP Client Peers yang ada, terjadi fluktuasi yang kurang lebih tidak jauh berbeda.

Berikut adalah diagram batang yang menggambarkan perbandingan tersebut:



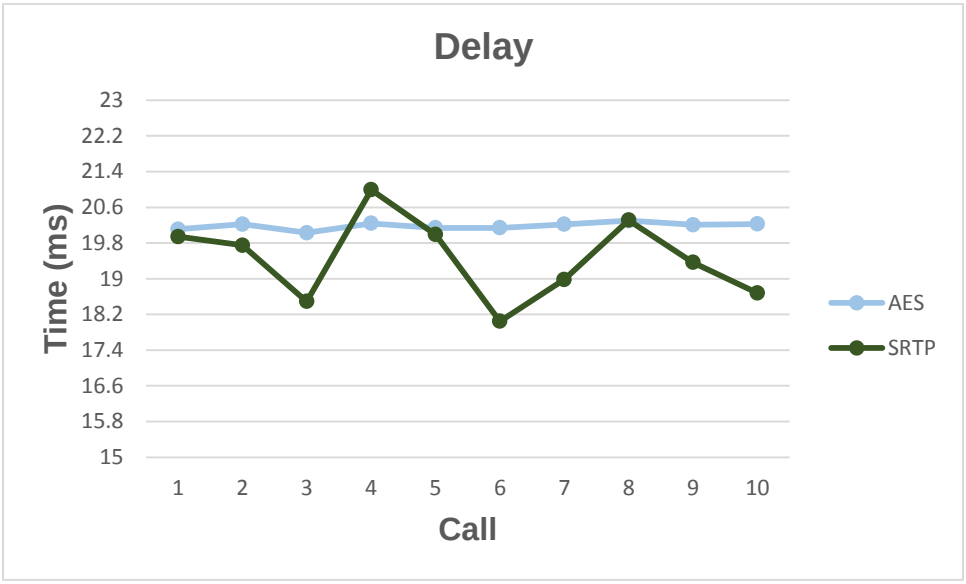
Gambar 16 Rata-rata *Throughput*

Gambar 16 di atas menunjukkan rata-rata penggunaan *throughput* yang dihasilkan berkisar antara 78.24 hingga 80.15 kbps. *Throughput* terbesar dimiliki oleh skema SRTP, sedangkan VoIP Client Peers yang diintegrasikan dengan menggunakan modul enkripsi AES dibawah SRTP dengan rata-rata 78.93 kbps.

Hasil yang diperoleh ini menunjukkan bahwa VoIP Client Peers dengan skema SRTP adalah VoIP Client Peers dengan performa terbaik, dengan asumsi semakin besar *throughput*, maka komunikasi antara pengguna VoIP akan semakin membaik.

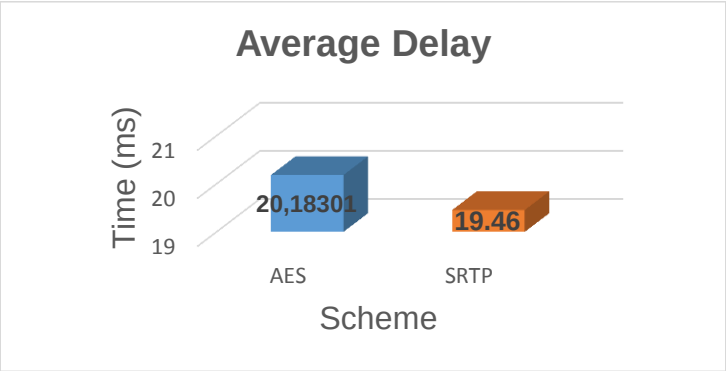
4.3. Hasil Pengujian *Delay*

Pengujian terakhir untuk mengukur kualitas dari layanan VoIP yaitu dengan menguji VoIP Client Peers menggunakan parameter *delay*. Dari pengujian yang dilakukan sebanyak 10 kali panggilan pada test bed, hasil dari pengukuran terhadap parameter delay ditunjukkan pada grafik dibawah ini:



Gambar 17 Hasil Pengukuran *Delay*

Hasil dari pengukuran yang dilakukan sebanyak 10 kali menunjukkan VoIP Client Peers dengan menggunakan skema SRTP memiliki *delay* yang paling kecil, sedangkan VoIP Client Peers dengan menggunakan modul enkripsi AES masih lebih tinggi bila dibandingkan dengan modul enkripsi SRTP. Sedangkan untuk rata-rata dari pengukuran delay akan ditunjukkan melalui diagram dibawah ini:



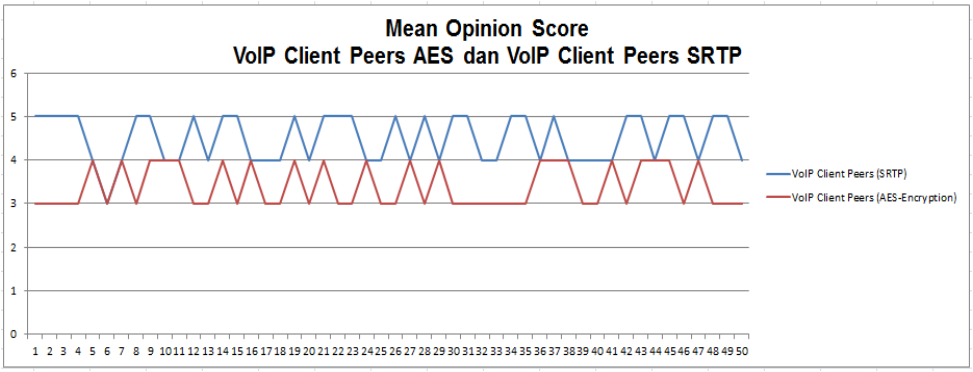
Gambar 18 Rata-rata *Delay*

Dari gambar 18 di atas terlihat bahwa rata-rata *delay* dari kedua skema menunjukkan bahwa VoIP Client Peers dengan menggunakan SRTP memiliki delay paling kecil yaitu 19.46 ms. Sedangkan VoIP client Peers yang diintegrasikan dengan modul enkripsi memiliki delay sebesar 20.18 ms.

Dari hasil yang ditunjukkan di atas, perbedaan selisih delay yang terjadi antara VoIP Client Peers yang diintegrasikan dengan modul enkripsi AES dan VoIP Client Peers yang menggunakan SRTP disebabkan terjadinya proses enkripsi pada setiap paket yang akan dikirim pada VoIP Client Peers dengan modul enkripsi. Jadi delay yang diukur yaitu delay pemrosesan dan bukan delay pada transmisi.

4.4. Pengujian Kualitas dengan *Mean Opinion Score* (MOS)

Dari 50 responden yang melakukan pengujian kualitas suara dari komunikasi yang dilakukan baik oleh VoIP Client Peers yang diintegrasikan dengan modul enkripsi maupun VoIP yang diintegrasikan dengan modul SRTP, maka didapatkan hasilnya sebagai berikut:

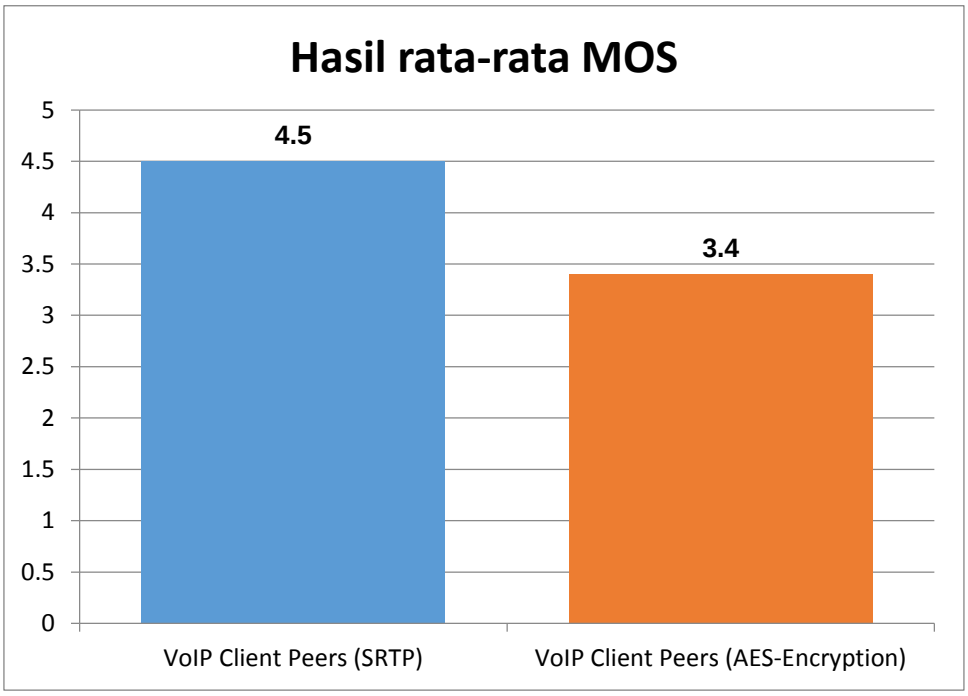


Gambar 19 Hasil Pengujian MOS

Dari grafik di atas dapat dilihat bahwa dari total 50 responden yang menguji dari kualitas komunikasi anatar kedua VoIP Client Peers tersebut menunjukkan VoIP

Client Peers yang diintegrasikan dengan modul SRTP memiliki performa yang paling baik di antara VoIP Client Peers yang diintegrasikan dengan modul enkripsi AES.

Dari tabel diatas maka bisa dibuat diagram batang untuk memudahkan melihat perbedaannya seperti dibawah ini:



Gambar 19 Hasil Rata-rata MOS

Dari diagram batang yang ditampilkan pada gambar 19 dapat dilihat bahwa setelah penulis menyebarkan kuesioner kepada 50 responden untuk menguji kualitas suara dalam komunikasi yang dihasilkan oleh VoIP Client Peers yang diintegrasikan dengan modul enkripsi AES dan juga VoIP Client Peers yang diintegrasikan dengan modul SRTP menunjukkan jika VoIP Client Peers yang diintegrasikan dengan modul SRTP memperoleh nilah 4,5, memiliki selisih 1,1 lebih baik bila dibandingkan dengan VoIP Client Peers yang diintegrasikan dengan modul enkripsi AES yang memperoleh nilah 3,4

Hasil ini dilatarbelakangi oleh suara yang dihasilkan VoIP Client Peers yang menggunakan modul enkripsi AES memiliki suara yang sedikit berisik (noise). Noise yang terjadi karena adanya pergeseran modulasi pada data digital yang disebabkan oleh waktu proses yang bertambah

4.5. Hasil dan Pembahasan

Dari hasil pengujian untuk mengukur layanan kualitas yang telah dilakukan didalam penelitian ini dengan menggunakan parameter yang sudah ditentukan antara lain *packet loss*, *delay*, dan *throughput* menunjukkan bahwa kinerja VoIP Client

Peers setelah diintegrasikan dengan modul enkripsi AES mengalami penambahan *delay processing* sebesar 0.72 ms bila dibandingkan dengan VoIP Client Peers dengan menggunakan SRTP.

Kemudian juga dari sisi *packet loss*, VoIP Client Peers yang diintegrasikan dengan modul enkripsi AES mempunyai jumlah paket yang hilang lebih tinggi sebesar 0.44% bila dibandingkan dengan VoIP Client Peers yang menggunakan modul SRTP

Dan *throughput* yang dihasilkan dari hasil pengujian pada lingkungan test bed menunjukkan bahwa VoIP Client Peers yang menggunakan modul SRTP memiliki throughput lebih besar sekitar 0.37% bila dibandingkan dengan VoIP yang diintegrasikan dengan modul enkripsi AES. Hal ini menunjukkan bahwa VoIP Client Peers yang menggunakan modul SRTp memiliki performa kinerja yang lebih baik bila dibandingkan dengan VoIP Client Peers yang sudah diintegrasikan dengan modul AES ataupun modul enkripsi lainnya.

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan uraian-uraian yang telah penulis jelaskan pada bab-bab sebelumnya, maka penulis dapat menarik beberapa kesimpulan sebagai berikut:

1. Modul enkripsi AES dan SRTP dapat diintegrasikan dengan baik pada VoIP Client Peers dengan mengenkripsi RTP Payload yang akan ditransmisikan pada jaringan VoIP.
2. Hipotesa awal yang digunakan pada penelitian ini menyatakan bahwa skema SRTP adalah skema enkripsi yang terbaik. Dan pada penelitian ini juga terbukti bahwa VoIP Client Peers dengan menggunakan skema SRTP memiliki kinerja yang terbaik.
3. Hasil pengujian MOS yang telah dilakukan pada penelitian ini menunjukkan bahwa VoIP Client Peers yang menggunakan modul SRTP mempunyai kualitas suara yang lebih baik bila dibandingkan dengan kualitas suara yang dihasilkan dari VoIP Client Peers yang diintegrasikan dengan menggunakan modul RTP AES Terenkripsi.

5.2. Saran

Dalam penelitian ini, adapun beberapa saran yang dapat diberikan untuk pengembangan penelitian ini anara lain:

1. Perlu adanya perbaikan kualitas suara yang dihasilkan dari VoIP Client Peers yang diintegrasikan dengan modul enkripsi
2. Adanya penambahan fitur “enable SRTP” pada VoIP client Peers yang diintegrasikan dengan modul SRTP agar pengguna dapat memilih antara menggunakan modul SRTp atau tidak dalam komunikasi pada jaringan VoIP.
3. Melakukan simulasi penyerangan didalam komunikasi VoIP Client Peers tersebut untuk menguji ketahanan data selama proses komunikasi yang berjalan.
4. Menganalisa data payload dari RTP yang telah dienkripsi.

DAFTAR PUSTAKA

1. Flower, Martin.2005.UML Distilled edisi 3.Panduan Singkat Bahasa Pemodelan Objek Standar. Yogyakarta : Andi.

2. Kelly, Timothy V.,. (2005). VoIP for Dummies. Indianapolis: Wiley Publishing, Inc. ISBN: 978-0-7645-8843-3

3. Muhammad Sarosa, Sigit Anggoro. 2000 . *Jaringan Komputer, Data Link, Network & Issue.* Jakarta.

4. Munir, Rinaldi. 2006. Kriptografi. Informatika. Jakarta

5. Passito, A., Mota, E., Mota, E. (2009). *Analysis of the Secure RTP Protocol on Voice over Wireless Networks using Extended MedQoS*.

6. Pressman, Roger S (2005). *Software Engineering: A Practiotiner's Approac* , Forth Edition, McGraw-Hill Book, Co.

7. Purbo, Onno w. 2007. *Cikal Bakal "Telkom Rakyat" (Paduan Lengkap Seting VOIP).* Mandiri Information System.2004. Membangun Jaringan LAN (buku 5). Mandiri Information System.

8. Shalahuddin, Muhammad dan Rosa Ariani S. 2007. *Belajar Pemrograman dengan bahada pemprograman C++ dan Java: Dari Nol menjadi Handal*. Penerbit Informatika.

9. T. Adomkus, E. Kalvaitis. (2008). *Investigation of VoIP Quality of Service using SRTP Protocol*.

10. Wahab, A. (2012). Analisis Kinerja VOIP Client Sipdroid dengan Modul Enkripsi Terintegrasi. ISSN: 1907-5022