ANALISIS KINERJA VOIP CLIENT SIPDROID DENGAN MODUL ENKRIPSI TERINTEGRASI

Rizal "Broer" Bahaweres[1] , Mudrik Alaydrus[2], Abdi Wahab[3]
[1,2,3]Jurusan Magister Teknik Elektro, Pascasarjana,Universitas Mercu Buana
Jl. Meruya Selatan, Kembangan, Jakarta 11650
E-mail: rizalbroer@ieee.org, mudrikalaydrus@yahoo.com, nangdul56@gmail.com

ABSTRAK
Jumlah pengguna VoIP di Indonesia masih kecil sekali, walaupun cost yang ditawarkan oleh VoIP lebih kecil dibandingkan dengan menggunakan telepon berpulsa. Salah satu alasannya adalah keamanan yang diberikan oleh penyedia layanan VoIP yang masih kurang. Pengguna VoIP belum mendapat layanan keamanan yang dapat menjamin keamanan komunikasi. Penelitian ini mencoba untuk mengamankan komunikasi antara pengguna VoIP dengan menggunakan modul enkripsi yang diintegrasikan dengan VoIP client Sipdroid yang berjalan di smartphone Android. Hal ini dimungkinkan oleh pengguna VoIP karena hanya VoIP client yang dapat diakses oleh pengguna VoIP. Hasil yang diperoleh setelah dilakukan integrasi dengan modul enkripsi menggunakan tiga buah skema enkripsi yaitu AES, DES, dan RC4, Sipdroid mampu menahan serangan pasif dari penyadapan informasi (eavesdropping) selama terjadi komunikasi. Dan hasil dari pengukuran QoS terdapat peningkatan delay sebesar 0.01 ms dan tidak terjadi perubahan yang signifikan terhadap througput dan packet loss, untuk throughput yang dihasilkan berkisar di 78 kbps, dan untuk packet loss rata-rata adalah 0.8 %. Akan tetapi terdapat noise yang mengikuti komunikasi pada Sipdroid yang terintegrasi dengan modul enkripsi akibat skew gelombang dari penambahan waktu proses ketika enkripsi.

Kata Kunci: VoIP, VoIP client, Enkripsi

1. PENDAHULUAN

1.1 Latar Belakang

Pengguna internet yang meningkat di Indonesia berdasarkan hasil survei dari Kominfo pada 2011 meningkat sangat pesat sekali. Prosentase terbesar 97.69% internet digunakan untuk mengirim dan menerima email, sedangkan paling rendah adalah promosi hotel diikuti oleh VoIP dengan masing-masing prosentase 0.14% dan 13.54%.

Jika dilihat dari hasil survei Kominfo penggunaan VoIP di Indonesia terbilang masih rendah, walaupun banyak referensi menyebutkan keunggulan VoIP dalam segi biaya lebih murah dibandingkan dengan dengan telepon konvensional. Selain memiliki keunggulan, VoIP juga terdapat kelemahan. Kelemahan yang masih sering terjadi adalah kualitas suara yang masih kurang baik jika dibandingkan dengan telepon konvensional. Selain kedua hal di atas, masalah keamanan juga menjadi banyak pertimbangan mengapa pengguna VoIP. Hal ini dikarenakan pengguna tidak mendapat jaminan yang baik dari penyedia jasa VoIP, kecuali perusahaan yang benar-benar komitmen untuk menyediakan jasa VoIP mungkin memiliki jaminan atas komunikasi yang dilakukan pengguna VoIP. Kemungkinan adanya penyerangan terhadap server VoIP dengan cara penyadapan (eavesdropping) bisa saja terjadi.

Pengguna VoIP tidak akan bisa mendapatkan akses dari server VoIP yang disediakan penyedia jasa VoIP, pengguna VoIP hanya bisa menggunakan VoIP client sebagai media komunikasi dan registrasi ke server VoIP. Mungkin cara untuk mengatasi masalah keamanan ini adalah dengan mengamankan data komunikasi yang akan dikirimkan dari VoIP client.

1.2 Tujuan dan Sasaran

Tujuan dari penelitian ini adalah mengintegrasikan modul atau fitur keamanan atau enkripsi data menggunakan beberapa metode enkripsi seperti AES, DES atau pun RC4 pada VoIP client Sipdroid saat melakukan komunikasi melalui VoIP. Dan juga untuk mengukur kinerja dari VoIP client yang telah diintegrasikan modul keamanan atau enkripsi.

Mendapatkan VoIP *client* yang telah diintegrasikan dengan modul enkripsi yang memiliki kinerja yang baik adalah sasaran dari penelitian ini. Dengan modul enkripsi yang diintegrasikan diharapkan dapat mengamankan komunikasi pengguna VoIP.

1.3 Perumusan Masalah

Perumusan masalah yang dapat ditentukan pada penelitian ini adalah sebagai berikut:

- Bagaimana mengintegrasikan VoIP client yang berjalan pada Smarthphone atau berbasis mobile dengan modul enkripsi?
- Bagaimana mengukur kinerja dari VoIP client berbasis mobile yang telah diintegrasikan dengan modul enkripsi?

1.4 Batasan Masalah

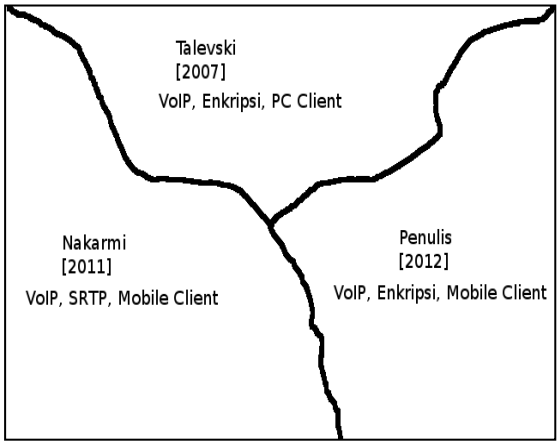
Batasan masalah pada penelitian ini adalah sebagai berikut:

a. Aplikasi VoIP client yang digunakan adalah Sipdroid.
b. Metode enkripsi yang coba diintegrasikan adalah AES, DES, dan RC4.
c. Test bed akan dilakukan pada lingkungan Android 2.3 (Ginger Bread).
d. Arsitektur jaringan menggunakan WLAN, sehingga lingkup komunikasi hanya dilakukan di dalam ruangan (indoor) saja.
e. Penelitian ini hanya sampai untuk mengintegrasikan modul enkripsi saja, tetapi belum dapat untuk memeriksa sampai dengan skema enkripsi yang digunakan ketika terjadi komunikasi.
f. Simulasi penyerangan yang dilakukan hanya sebagai serangan pasif atau serangan yang hanya untuk mendengarkan informasi yang ada selama komunikasi (eavesdropping).
g. Penelitian ini belum sampai memeriksa perubahan data komunikasi yang terjadi akibat dari proses enkripsi.

2. KAJIAN PUSTAKA

2.1 Penelitian Terkait

Penulis mendapatkan beberapa penelitian lama yang terkait dengan penelitian ini. Pada penelitian yang dilakukan oleh Talevski et al (2007), pada tulisannya yang berjudul "Secure Mobile VoIP", dan juga penelitian Nakarmi et al (2011). Perbedaan dari penelitian penulis dengan kedua penelitian sebelumnya digambarkan penulis pada Gambar 1 berikut.



Gambar 1. Penggambaran Penelitian Terkait dengan Peneltian ini.

Talevski mencoba menambahkan modul enkripsi pada VoIP client Kiax. Kiax adalah salah satu VoIP client yang menggunakan protokol IAX (Inter-Asterisk Exchange), yang menyerupai protokol SIP dan H323. Talevski mengintegrasikan Kiax dengan modul enkripsi yang dihasilkan menggunakan kepustakaan Cryptlib. Cryptlib berisi fungsi-fungsi kriptografi yang dapat diintegrasikan dengan aplikasi. Skema enkripsi yang digunakan oleh Talevski adalah IDEA, RC4, dan AES. Kemudian, dari hasil Kiax yang diintegrasikan dengan modul enkripsi diuji pada jaringan VoIP menggunakan LAN. Parameter yang diambil adalah delay, jitter, bandwidth, dan kinerja CPU. Dari hasil yang didapat pada penelitian Talevski, Kiax dengan skema AES CFB adalah yang skema yang dipilih dibandingkan dengan skema lain yang diuji.

Penelitian lain yang berhubungan dengan penelitian ini adalah penelitian Nakarmi et al [2011] yang berjudul "Evaluation of VoIP Media Security for Smartphones in The Context of IMS". Pada penelitian tersebut, Nakarmi mengeksplorasi alternatif dan kelayakan untuk mendapatkan keamanan media VoIP untuk smartphone di lingkup dari IP Multimedia Subsystem (IMS). Pada penelitian tersebut, Nakarmi merubah Sipdroid menjadi menggunakan SRTP dan juga MICKEY-TICKET. SRTP adalah Secure Real Time Protocol, dan MICKEY-TICKET adalah protokol untuk pertukaran kunci.

2.2 Sipdroid

Sipdroid adalah sebuah voip client yang berjalan sistem operasi Android. Sipdroid menggunakan lisensi *GNU Public License* (GPL) v3, dan dapat diunduh secara gratis dari Android *Market* atau juga dari website Sipdroid yaitu http://sipdroid.org. Pada website tersebut juga dapat diunduh untuk sumber Sipdroid bagi pengguna yang ingin memodifikasi atau mengkompilasi ulang Sipdroid.

Sipdroid menggunakan protokol SIP (*Session Initiation Protocol*) sebagai pengatur inisiasi sesi multimedia. Dan untuk implementasinya Sipdroid menggunakan kepustakaan MjSip.

2.3 Java Crypthography Extention (JCE).

JCE menyediakan *framework* dan implementasi untuk algoritma pengenkripsian, pembangkit kunci (*key generation*) dan (*key agreement*), dan kode otentikasi pesan (*message authentication code*).

Mendukung enkripsi *symmetric*, *asymmetric*, *block*, dan *stream cipher*. Juga mendukung *secure stream* dan *sealed object*.

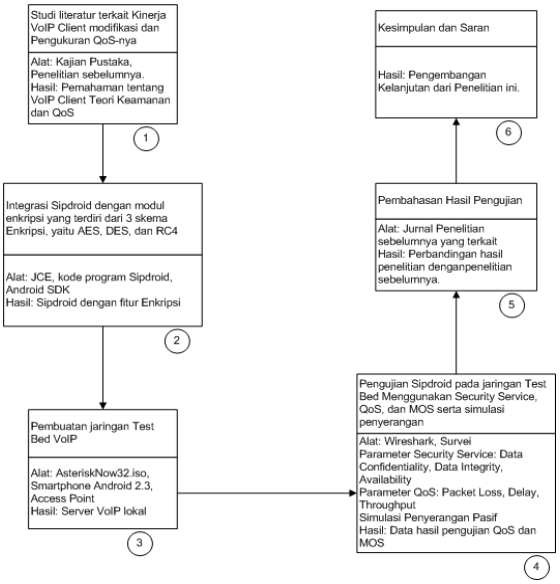
JCE API meliputi:

- Enkripsi *symmetric* yang besar, seperti DES, RC2, dan IDEA.
- Enkripsi symmetric stream, seperti RC4.
- Enkripsi asymmetric, seperti RSA.
- Enkripsi berbasis password (Password-based Encryption).
- Key Agreement.
- Message Authentication Code (MAC).

Beberapa konsep dasar kriptografi yang penulis gunakan pada penelitian ini, penulis ambil dari buku Stalling (2005).

3. METODOLOGI PENELITIAN

Metodologi penelitian yang peneliti coba lakukan adalah sebagai berikut:



Gambar 2. Metodologi Penelitian

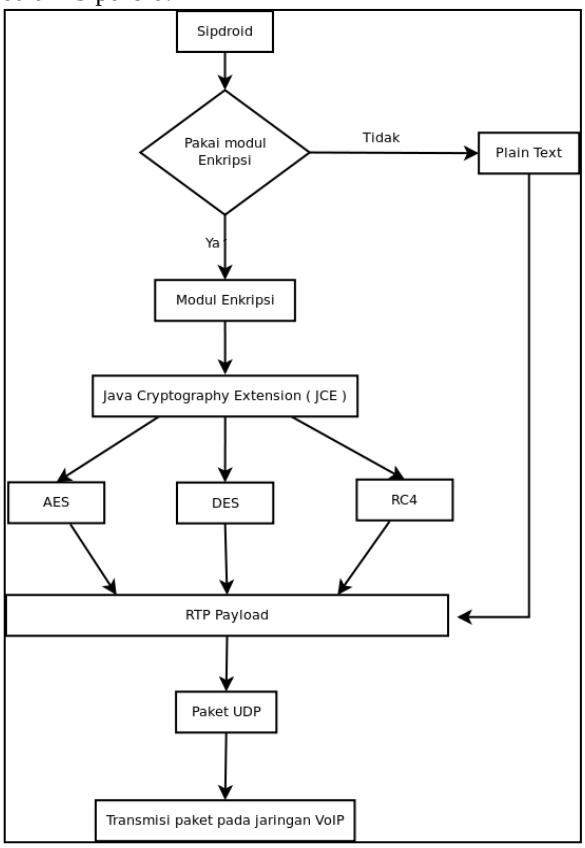
Metodologi yang digunakan diawali dengan menggunakan studi literatur terhadap penelitian yang terkait, kemudian mengintegrasikan modul enkripsi dengan Sipdroid, pembuatan jaringan test bed untuk VoIP, Pengujian Sipdroid hasil integrasi dengan modul enkripsi, pembahasan hasil pengujian, dan terakhir adalah pengambilan kesimpulan dan saran.

Tabel 1. Korelasi antara metode, perangkat, parameter dan hasil

No	Metode / Teknik	Perangkat	Parameter	Hasil
1.	Pembuatan skema enkripsi AES, DES, RC4	JCE	Kunci, Data	Modul Enkripsi dengan AES, DES, RC4.
2.	Integrasi Sipdroid dengan Modul Enkripsi	Modul Enkripsi, Source Sipdroid		Sipdroid yang terintegrasi dengan fitur enkripsi.
3.	Pembuatan Jaringan Test bed	Smartphone Android, Server VoIP dengan Asterisk		Test bed jaringan VoIP.
4.	Pengujian Sipdroid dengan fitur enkripsi menggunakan Layanan Keamanan.	Test bed jaringan VoIP, Smartphone Android, Wireshark	Data Confidentiality, data integrity, availability	Data pengujian dengan Layanan Keamanan.
5.	Pengukuran kinerja Sipdroid dengan fitur enkripsi.	Wireshark, Test bed jaringan VoIP, Smartphone Android, survei.	Delay, packet loss, throughput, MOS.	Data pengukuran kinerja Sipdroid

3.1 Integrasi Sipdroid dengan Modul Enkripsi

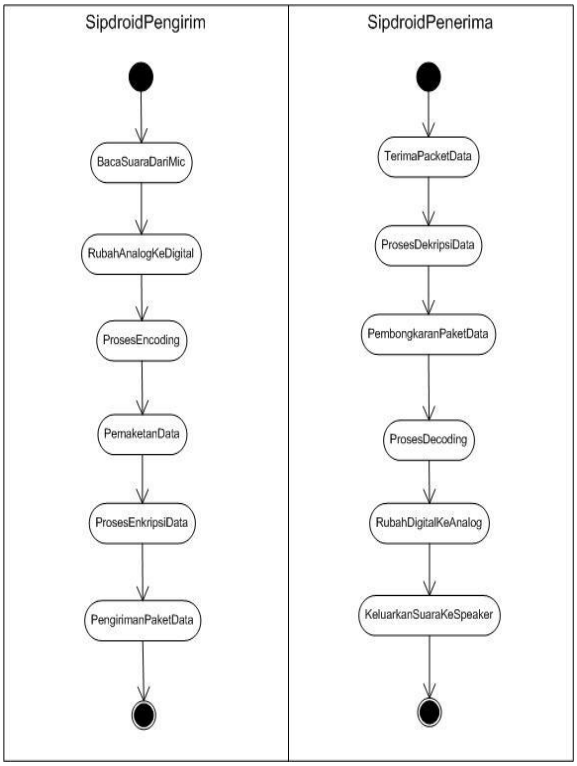
Selanjutnya peneliti akan mengintegrasikan antara Sipdroid dengan modul enkripsi yang dihasilkan menggunakan JCE. Berikut adalah penggambaran proses integrasi modul enkripsi ke dalam Sipdroid.



Gambar 3. Proses integrasi JCE dengan Sipdroid

Tahapan proses pada Gambar 2, pengguna dapat memilih apakah menggunakan modul enkripsi atau tidak menggunakan modul enkripsi. Jika menggunakan modul enkripsi, maka pengguna memilih salah satu metode enkripsi, yaitu AES, DES, dan RC4. Proses enkripsi dilakukan pada RTP payload sebelum RTP dibungkus menjadi paket UDP dan dikirim melalui jaringan VoIP.

Sehingga aktifitas dari Sipdroid berubah menjadi seperti gambar berikut.

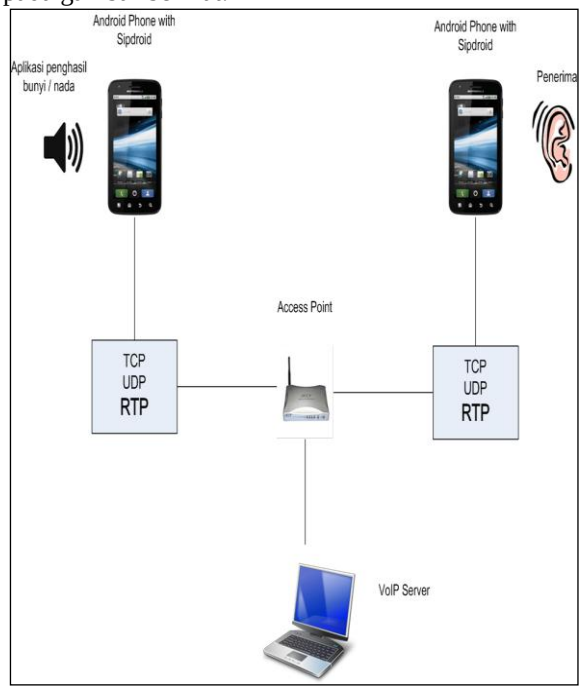


Gambar 4. Diagram aktifitas Sipdroid hasil modifikasi

Pada Sipdroid pengirim terdapat proses enkripsi data pada paket RTP yang akan dikirimkan, sedangkan pada Sipdroid penerima terjadi proses dekripsi data pada paket RTP yang diterima.

3.2 Perancangan Test Bed untuk VoIP

Test bed yang akan penulis bangun digambarkan pada gambar berikut.



Gambar 5. Test bed jaringan VoIP

Test bed yang akan digunakan hanya terdiri dari dua buah smatrphone Android, yang melakukan komunikasi melalui sebuah server VoIP yang dibangun sendiri. Jaringan yang digunakan menggunakan WLAN. Untuk pengukuran, agar suara yang dihasilkan sama, maka digunakan aplikasi penghasil nada agar dapat dilakukan pembuatan nada secara otomatisasi.

3.3 Skenario Pengujian

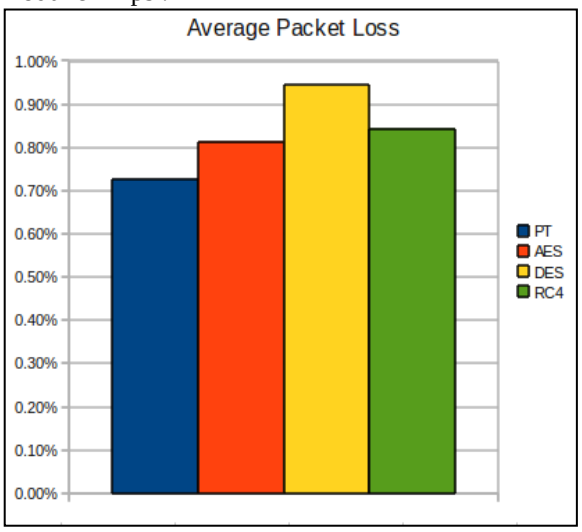
Skenario pengujian pertama menggunakan parameter delay, packet loss, dan juga throughput, yang penulis ambil dari buku Stalling (2004). Pengukuran di lakukan pada *end-to-end* atau di setiap smartphone Android menggunakan alat bantu Shark. Pengambilan data dilakukan sebanyak dua puluh kali untuk setiap skema enkripsi dengan menggunakan kunci yang sama, dan setiap sesi komunikasi dilakukan selama 15 detik. Komunikasi hanya terjadi dalam satu arah, dan suara yang dihasilkan menggunakan bantuan aplikasi sebagaimana yang tergambar pada Gambar 5.

4. HASIL DAN PEMBAHASAN

Berikut adalah hasil yang diperoleh pada penelitian ini, menggunakan parameter-parameter yang telah disebutkan pada sub bab 3.3.

4.1 Packet Loss

Berikut adalah rata-rata packet loss yang didapat dari pengukuran Sipdroid yang terintegrasi dengan modul enkripsi.



Gambar 6. Rata-rata Packet Loss

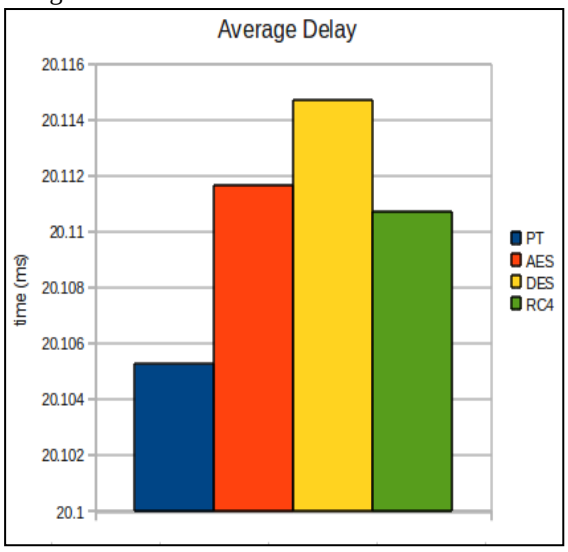
Hasil Gambar 6 di atas menggambarkan bahwa Sipdroid normal memiliki rata-rata packet loss paling kecil dibandingkan dengan Sipdroid yang diintegrasikan dengan modul enkripsi. Sedangkan Sipdroid dengan skema DES memiliki packet loss terbesar dibandingkan dengan yang lain. Sehingga performa yang terbaik masih dipegang Sipdroid normal, diikuti oleh Sipdroid dengan skema AES, diposisi ketiga Sipdroid dengan skema RC4, dan

terakhir yang menampilkan performa yang kurang baik adalah DES. Pada dasarnya, komunikasi pada VoIP terlebih lagi yang menggunakan jaringan Wireless akan menghasilkan packet loss.

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

4.2 Delay

Hasil rata-rata yang diperoleh selama pengukuran delay (delay pembuatan packet) adalah sebagai berikut.



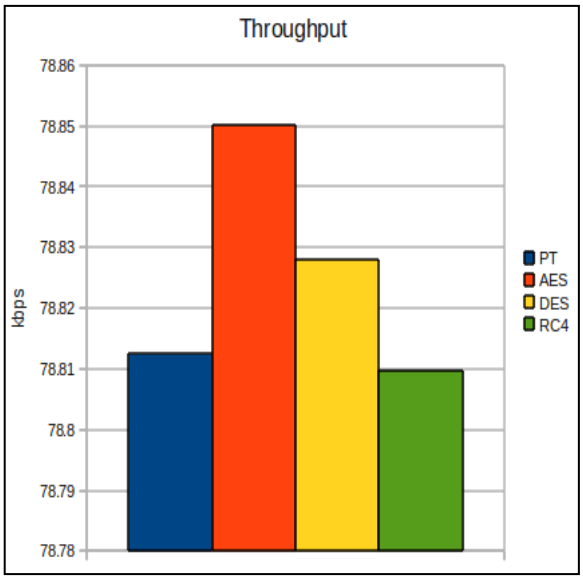
Gambar 7. Rata-rata Delay

Gambar 7 di atas menunjukkan rata-rata delay dari empat buah skema yang penulis uji. Sipdroid normal memiliki rata-rata delay paling kecil dibandingkan dengan Sipdroid dengan modul enkripsi. Perbedaan delay yang terjadi sekitar 0.01 ms untuk penambahan pada Sipdroid dengan modul enkripsi. Sedangkan di antara Sipdroid dengan modul enkripsi, Sipdroid dengan skema AES dan RC4 memiliki delay yang tidak jauh berbeda, dan untuk Sipdroid dengan skema DES memiliki delay yang paling besar.

Dari hasil yang ditunjukkan di atas, perbedaan selisih delay yang terjadi antara Sipdroid normal dengan Sipdroid dengan modul enkripsi disebabkan terjadinya proses enkripsi pada setiap paket yang akan dikirimkan pada Sipdroid dengan modul enkripsi. Jadi delay yang penulis ukur adalah delay pemrosesan, bukan delay transmisi.

4.3 Throughput

Rata-rata throughput yang dihasilkan pada pengukuran ini adalah sebagai berikut.



Gambar 8. Rata-rata Throughput

Gambar 8 di atas, menunjukkan penggunaan throughput yang dipakai pada skema Sipdroid yang diuji. Rata-rata *throughput* yang dihasilkan berkisar di angka 78 kbps. Throughput terbesar dimiliki Sipdroid dengan skema AES, sedangkan Sipdroid normal memiliki *throughput* yang tidak jauh berbeda dibandingkan dengan Sipdroid dengan skema RC4. Sedangkan Sipdroid dengan skema DES berada di bawah dari Sipdroid dengan skema AES, atau menempati urutan ke dua teratas. Perbedaan throughput ini disebabkan pada proses enkripsi atau algoritma enkripsi yang digunakan, pada proses ini terjadi pembentukan paket dengan bit yang lebih besar dari bit yang biasa, terutama pada hasil paket yang dihasilkan dari Sipdroid AES dan DES yang masing-masing merubah panjang paket menjadi 128 dan 64 bit.

Hasil yang peneliti peroleh pada pengukuran *throughput* ini, di antara Sipdroid yang diintegrasikan dengan modul enkripsi, Sipdroid dengan skema AES adalah performa terbaik, dengan asumsi, semakin besar throughput, maka komunikasi antara pengguna VoIP akan semakin baik. Tapi hal ini tidak terjadi pada Sipdroid normal, pada Sipdroid normal, terjadi komunikasi yang baik antara pengguna VoIP ketika melakukan komunikasi walaupun throughput yang dihasilkan lebih kecil dibandingkan dengan Sipdroid dengan skema AES.

4.4 Pembahasan

Hasil yang diperoleh dari penelitian ini, terutama dari ketiga pengukuran parameter kualitas layanan (QoS), yaitu delay, packet loss, dan throughput, skema enkripsi yang peneliti ajukan untuk digunakan adalah skema AES, walaupun masih terdapat noise yang dihasilkan dari proses enkripsi tersebut.

Pada awal penelitian ini, peneliti akan mencoba melakukan simulasi penyerangan yang akan

dilakukan pada Sipdroid yang terintegrasi dengan modul enkripsi sebagaimana pada Gambar 5. Akan tetapi, karena keterbatasan waktu, alat dan tempat, maka simulasi penyerangan akan penulis lanjutkan pada penelitian berikutnya.

5. KESIMPULAN DAN SARAN

Kesimpulan pada penelitian ini adalah sebagai berikut

- Modul enkripsi yang dihasilkan dari JCE dapat diintegrasikan dengan baik pada Sipdroid dengan mengenkripsi RTP payload yang akan ditransmisikan pada jaringan VoIP.
- Pengukuran kinerja dari Sipdroid yang terintegrasi dengan modul enkripsi menggunakan parameter kualitas layanan (QoS), yaitu delay, packet loss, dan throughput, menghasilakan delay yang membesar lebih dari 0.01 ms pada Sipdroid dengan modul enkripsi, sedangkan pada packet loss dan throughput tidak terjadi perubahan yang signifikan.
- Sipdroid dengan modul enkripsi menurut analisa penulis mampu mengatasi dari penyerangan pasif yang bersifat mendengarkan informasi (eavesdropping) pada komunikasi VoIP yang dilakukan.

Sedangkan saran yang dapat diberikan pada penelitian ini adalah sebagai berikut.

- Melakukan simulasi penyerangan terhadap Sipdroid dengan pengintegrasian modul enkripsi.
- Memperbaiki kualitas suara dari Sipdroid yang diintegrasikan dengan modul enkripsi.
- Menambahkan modul untuk mengetahui skema enkripsi pada awal proses komunikasi pada VoIP, sehingga jika skema enkripsi yang dipakai berbeda maka komunikasi langsung terputus.
- Menganalisa data payload dari RTP yang telah dienkripsi.

DAFTAR PUSTAKA

Amin, A. H. M. (2005). VoIP Performance Measurement Using QoS Parameter. International Converence on IIT, Dubai, UEA.

Nakarmi, P.K., Mattsson, J., & Maguire, G.Q. (2011). Evaluation of VoIP Media Security for Smartphones in the Context of IMS. Paper pada Swedish Communication Technologies Workshop, Stockholm, Swedia.

Purbo, O. W., & Raharja, A. (2010). VoIP Cookbook. [On-line] Diakses di http://opensource.telkomspeedy.com/wiki/index.php/VoIP_Cookbook:_Building_your_own_Telecommunication_Infrastructure pada 20 Januari 2012.

Schildt, H. (2002). Java 2: The Complete Reference, Fifth Edition. New York: McGraw Hill.

Stalling, W. (2004). Computer Networking with Internet Protocols and Technology. Upper Sadle River: Prentice Hall.

Stallling, W. (2005). Crypthography and Network Security Priciples and Practices, Fourth Edition. Upper Sadle River: Prentice Hall.

Talevski, A., Chang, E., & Dillon, T. (2007). Secure Mobile VoIP. Paper pada International Converence on Convergence Information Technology, Gyeongju, Korea.

----------. Hasil Survei Penggunaan Teknologi Informasi dan Komunikasi (TIK) di Sektor Bisnis Indonesia 2011. [On-line] Diakses di http://publikasi.kominfo.go.id/bitstream/handle/54323613/66/Hasil%20Survei%20TIK%20Sektor%20Bisnis%202011.pdf?sequence=1 pada 15 Februari 2012.