Analisis *Quality of Services* Jaringan *VoIP* pada *VPN* menggunakan *InterAsteriks Exchange* dan *Session Initiation Protocol*

Quality of Services Analysis of VoIP Networks over VPN using InterAsteriks Exchange and Session Initiation Protocol

Agus Heriyanto[1], Lailis Syafaah[2], Amrul Faruq[3]
[1,2,3]Jurusan Teknik Elektro, Fakultas Teknik, Universitas Muhammadiyah Malang
E-mail: faruq@umm.ac.id

Abstrak

Di dalam komunikasi *Voice over Internet Protocol (VoIP)* mengenal beberapa macam *protocol* tambahan selain *protocol* standar *internet Transfer Control Protocol/Internet Protocol (TCP/IP)*, beberapa diantaranya adalah *protocol Session Initation Protocol (SIP), Inter-Asterisk eXchange (IAX)* dan *H.323*. Performansi perlu dijaga mengingat *VoIP* mempunyai kemungkinan melakukan berbagai cara kompresi untuk menciptakan efisiensi saluran dan pemilihan *protocol* yang tepat. Teknologi *VoIP* pada dasarnya tidak memiliki jaminan keamanan pada setiap komunikasi. Keamanan ketika melakukan komunikasi suara merupakan sesuatu yang sangat penting karena menyangkut privasi penggunanya. Penggunaan *Virtual Private Network (VPN)* merupakan salah satu solusi untuk menutup celah keamanan pada kasus di atas. Analisis yang dilakukan pada artikel ini adalah performa yang dihasilkan *VoIP* yang menggunakan *protocol IAX* dan *SIP*. Penelitian ini mengahasilkan kesimpulan bahwa performansi yang paling baik digunakan untuk membangun sistem komunikasi *VoIP* adalah *protocol IAX* dengan menggunakan sistem keamanan *VPN Point to Point Protocol (PPTP)* dikarenakan nilai *Quality of Service (QoS)* lebih tinggi daripada *protocol SIP* dan juga terbukti lebih aman saat diterapkan sistem keamanan *Virtual Private Network Point to Point Protocol (VPN PPTP).*

Kata kunci: Voice over *Internet Protocol*, Quality of Services, Virtual Private Network, *SIP*, *IAX*

Abstract

In VoIP communication, there are several additional protocols beside the standard TCP/IP protocols, some of them are the Session Initation Protocol (SIP), Inter-Asterisk eXchange (IAX), and H.323. Performance needs to be maintained given that VoIP has the possibility to perform various compression methods to create channel efficiency and selection of the right protocol. VoIP technology basically does not have a guarantee of security on every communication. Security when conducting voice communication is something that is very important due to it involves the privacy of its users. The use of a Virtual Private Network (VPN) is one solution to close the security gap in the case mentioned. The analysis carried out in this article is the performance produced by VoIP using the IAX and SIP protocols. In this study concluded that the best performance used to build a VoIP communication system is the IAX Protocol using a Point to Point Protocol (PPTP) security system because the Quality of Service (QoS) value is higher than the SIP protocol and also proved to be safer when applied PPTP VPN security system.

Keywords: Voice over Internet Protocol, Quality of Services, Virtual Private Network, SIP, IAX

1. PENDAHULUAN

Dewasa ini perkembangan teknologi yang sangat pesat mendorong terbentuknya suatu komunikasi yang bersifat *convergence* dengan teknologi komunikasi lainnya. Salah satunya adalah *Voice over Internet Protocol (VoIP). VoIP* merupakan teknologi yang menawarkan layanan transmisi data suara, video, dan data secara langsung atau *real time* melalui *internet* yang berjalan pada suatu *protocol* jaringan komputer yaitu *Internet Protocol (IP)*. Teknologi *VoIP* merupakan teknologi yang dapat mengkonversi suara menjadi *signal* digital dan kemudian ditransmisikan menjadi paket-paket data yang bekerja pada *protocol IP* [1]. Penggunaan jaringan IP memungkinkan penghematan biaya, karena tidak perlu membangun sebuah infrastruktur baru untuk komunikasi suara dan penggunaan *bandwith* yang lebih kecil dibandingkan telepon biasa. Teknologi ini *(VoIP)* dapat dikembangkan sedemikian rupa sesuai dengan keinginan dan biaya penggunaan yang murah serta banyak keuntungan yang dapat diambil [2].

Dalam pengoperasiannya, *VoIP* memiliki *protocol* yang merupakan sebuah aturan yang harus dipenuhi agar akses komunikasi dalam hal ini komunikasi *VoIP* dapat melewati jaringan. Di dalam komunikasi *VoIP* mengenal beberapa macam *protocol* tambahan selain *protocol* standar *internet TCP/IP*, beberapa diantaranya adalah *protocol SIP*, *IAX* dan *H.323*. *Session Initiation Protocol (SIP)* adalah *protocol* yang dikembangkan oleh *Internet Engineering Task Force (IETF),* kemudian *IAX* atau singkatan dari *Inter Asterisk eXchange* adalah *protocol* yang dibuat dan dikembangkan oleh komunitas Asterisk, sedangkan *H.323* adalah *protocol* yang di rekomendasikan oleh *ITU Telecommunication Standardization Sector (ITU-T)* [3].

Pada penelitian sebelumnya dapat kita ketahui hasil dari performansi *VoIP* yang menggunakan *protocol SIP* seperti pada hasil pengujian kualitas suara pada *VoIP Computer to Computer* Berbasis *Freeware* Menggunakan *Session Initiation Protocol* [4] dan pada pekerjaan yang lain implementasi *VoIP SIP* Pada *Mobile Phone* di Jaringan *Bluetooth* [5]. Secara umum sistem *VoIP* yang menggunakan *protocol SIP* dapat beroperasi dengan baik serta memiliki kualitas suara yang cukup memuaskan. Dikarenakan *Protocol VoIP* tidak hanya *SIP* saja, maka dari itu pekerjaan ini mengeksplorasi *protocol-protocol* lainnya pada *VoIP* agar dapat dijadikan pengambilan keputusan untuk menentukan *protocol* mana yang terbaik pada perancangan sistem *VoIP* yang dibangun [6]. Lebih jauh lagi, penelitian [7] menyajikan simulasi jaringan *SIP* real time dan sistem pemantauan *(monitoring)*. Simulator jaringan *SIP* didasarkan pada model generatif probabilistik yang meniru jaringan sosial pelanggan *VoIP* yang saling memanggil secara acak. Sistem pemantauan, dipasang di *server SIP*, menyediakan layanan untuk mengumpulkan data jaringan dan statistik *server* secara real time. Sistem ini menyediakan kerangka kerja yang kuat untuk mengembangkan aplikasi jaringan *SIP* seperti monitor keamanan.

Performansi perlu dijaga mengingat *VoIP* mempunyai kemungkinan melakukan berbagai cara kompresi untuk menciptakan efisiensi saluran dan pemilihan *protocol* yang tepat. Belum lagi dengan jaminan keamanan terhadap setiap paket data pada setiap komunikasi suara yang dilakukan. Teknologi *VoIP* pada dasarnya tidak memiliki jaminan keamanan pada setiap komunikasi. Karena penggunaan komunikasi yang murah dari sisi keamanan kurang begitu diperhatikan. Hal ini disebabkan karena media transmisi paket data yang melalui *unprotected network* pada jaringan *internet*. Sehingga memungkinkan penyadapan atau peretasan komunikasi suara maupun data-data oleh pihak yang tidak bertanggungjawab. Salah satu kelemahan jaringan *internet* adalah bahwa data yang terkirim tidak terjamin kerahasiaannya sehingga siapapun dapat mengambildan memanipulasi data tersebut [1].

Setiap komunikasi antar *user* yang melalui jaringan *internet* dapat dilakukan penyadapan, sehingga percakapan antar *user* dapat diretas atau disadap. Hal ini ditakutkan jika ada pihak yang tidak bertanggung jawab mencuri informasi yang beredar. Tentunya hal ini dapat menjadi kerugian bagi *user* tersebut [8]. Pada referensi [9], implementasi keamanan jaringan komunikasi *VoIP* berbasis *protocol SIP* berhasil dilakukan. Artikel tersebut menyajikan hasil arsitektur konkret dan layak untuk mengamankan panggilan *VoIP*. Sementara itu,

kaitannya dengan keamanan jaringan, *VoIP* pada jaringan *Internet Protocol* versi 6 (IPv6) juga sudah dianalisa dengan system tunnelling [10].

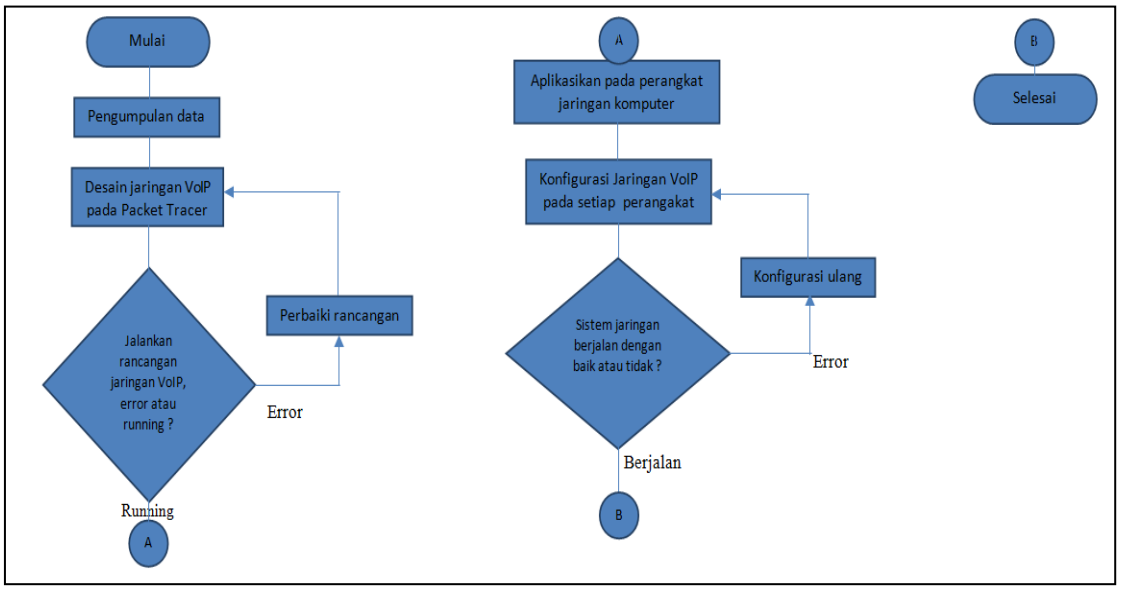
Oleh karena itu, keamanan ketika melakukan komunikasi suara merupakan sesuatu yang sangat penting karena menyangkut privasi penggunanya pada arsitektur *VoIP*. Penggunaan *Virtual Private Network* (*VPN*) merupakan salah satu solusi untuk menutup celah keamanan pada kasus di atas. *VPN* merupakan salah satu alternatif untuk mengirimkan data dan suara, yang bersifat *private* atau aman [11]. Menyatukan *VoIP* dengan *Internet of Things* (IoT) teknologi merupakan skema baru yang dapat dijadikan alternatif keamanan jaringan *VoIP* terhadap potensi ancaman [12]. Pada artikel ini bertujuan untuk investigasi performa yang dihasilkan *VoIP* yang menggunakan *protocol SIP* dan *IAX* sekaligus mengevaluasi penggunaan keduanya dengan mengukur tingkat *Quality of Services*. Kemudian dilakukan analisis pada performa *VoIP* tanpa *VPN* dengan *VoIP* yang menerapkan *VPN* pada saat jaringan sibuk dan atau pada saat jaringan lenggang. Selain itu juga perlu dipertimbangkan terkirimnya data secara *real-time* agar tercapainya *Quality of Service* (QoS) pada jaringan *VoIP* yang digunakan.

2. METODE PENELITIAN

Pekerjaan ini menggunakan pendekatan penelitian eksperimental. Penelitian eksperimental adalah penelitian yang dilakukan dengan menciptakan fenomena pada kondisi terkendali. Penelitian ini bertujuan untuk menemukan perbandingan dan pengaruh faktor-faktor pada kondisi tertentu. Penelitian ini berupaya menjelaskan perbandingan antara dua *protocol* berbeda pada sebuah sistem telekomunikasi yang sama yaitu *Voice over Internet Protocol* (*VoIP*) dari segi performansi dan keamanan sebuah *protocol* yang diterapkan. *Protocol* yang dianalisa adalah *protocol IAX* dan *protocol SIP* dengan tambahan sistem keamanan *VPN* pada masing-masing implementasinya.

2.1 Diagram Alir Perancangan Sistem

Untuk melakukan penelitian pada Analisis Performansi dan Keamanan *Voice over Internet Protocol* (*VoIP*) Pada Jaringan *Virtual Private Network* (*VPN*) Berbasis *Protocol Inter-Asterisk eXchange* (*IAX*), dapat dilakukan dengan beberapa langkah seperti terlihat dalam gambar 1. Blok diagram penelitian seperti dilihatkan pada Gambar 2. Sedangkan topologi jaringan *VoIP* yang dibangun pada pekerjaan ini dapat dilihat pada Gambar 3.

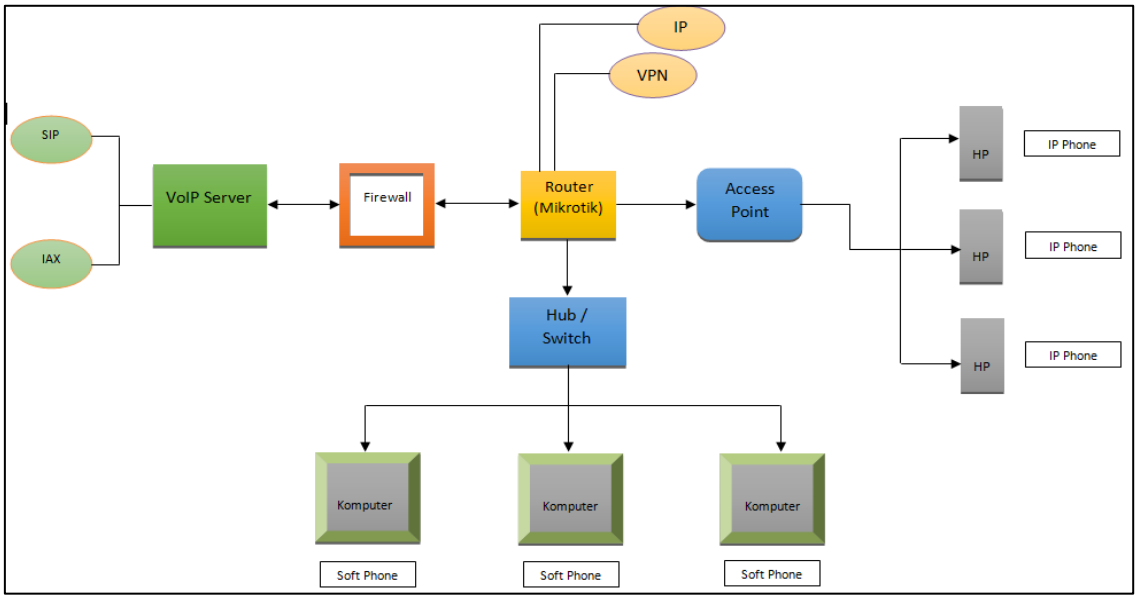


Gambar 1 Diagram Alir Perencanaan Jaringan *VoIP*

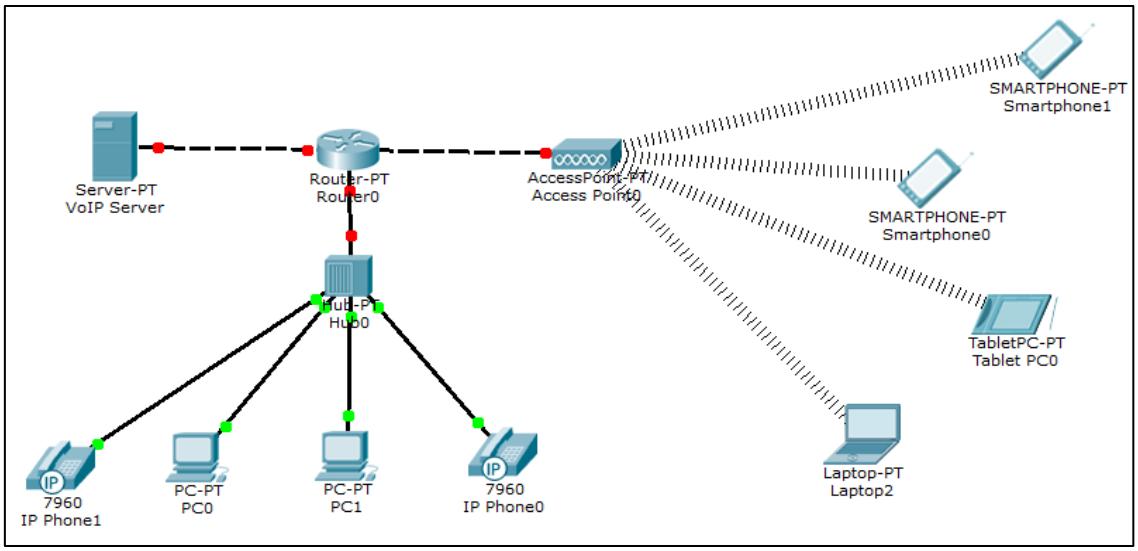
2.2 Cara Kerja dan Pengujian

a. Instalasi sistem operasi pada *server VoIP*

Instalasi sistem operasi *VoIP server* pada penelitian ini dengan menggunakan *Open Source Linux Free PBX*. Alasan penulis menggunakan sistem operasi *FreePBX* karena sistem operasi ini mudah dikonfigurasi dikarenakan sudah mendukung *Graphical User Interface* (GUI) dan dapat menggunakan *multi protocol* tanpa harus meng*instal* ulang atau mengkonfigurasi kembali ketika ingin berpindah atau berganti *protocol* yang akan diterapkan [13].



Gambar 2 Blok Diagram Sistem *VoIP*



Gambar 3 Emulasi Topologi Jaringan *VoIP*

b. Konfigurasi *server VoIP*

Konfigurasi pada *VoIP server* ada 3 yaitu berturut-turut meliputi konfigurasi *protocol* standar, konfigurasi *protocol VoIP*, dan konfigurasi *user* pada *VoIP server*.

c. Konfigurasi pada router Mikrotik

Pada perangkat *router* dibutuhkan konfigurasi untuk mengatur lalu-lintas jaringan

antara *server* dan *user*. Konfigurasi pada *router* adalah sebagai berikut meliputi *Ethernet, Internet Protocol* (IP), konfigurasi *Dynamic Host Configuration Protocol (DHCP) server, VPN point to point protocol* (*PPTP*) [14].

d. Konfigurasi pada *Access Point* IP *Service Set Identifier (SSID) Password Wi-Fi DHCP Server*
e. Konfigurasi pada *user*

Konfigurasi pada perangkat yang digunakan *user* terbagi dua yaitu pada perangkat komputer/*laptop* instalasi dan konfigurasi *softphone Zoiper*, dan konfigurasi *VPN client* dan pada perangkat *smartphone* meliputi instalasi dan konfigurasi *softphone Zoiper*

3. HASIL DAN PEMBAHASAN

Dalam pembuatan sistem jaringan *VoIP* untuk menganalisa performansi dan keamanannya dilakukan prosedur operasi dan pengujian yang mengacu pada desain perancangan hal ini dijelaskan dengan beberapa tahap yang harus dilakukan seperti yang telah diterangkan pada bagian sebelumnya. Uji paramater-parameter yang mempengaruhi performansi *Quality of Services (QoS)* pada jaringan IP yang dibatasi pada masalah seperti ditunjukkan dalam persamaan (1) sampai dengan persamaan (4), yang masing-masing adalah *Throughput*, *Jitter*, *Packet loss* dan *Delay*.

$$Throughput = \frac{Paket\ Data\ Yang\ Diterima}{Lama\ Pengamatan} \quad (1)$$

$$Jitter = \frac{Total\ Variasi\ Delay}{Paket\ Yang\ Diterima} \quad (2)$$

$$P.Loss = \frac{Paket\ Data\ Terkirim - Paket\ Data\ Diterima}{Paket\ Data\ Terkirim}\ x\ 100\% \quad (3)$$

$$Delay\ Rata - Rata = \frac{Lama\ Pengamatan}{Total\ Paket\ Yang\ Diterima} \ldots . \quad (4)$$

Hasil uji performansi *VoIP* dengan *protocol IAX* tanpa menggunakan keamanan *VPN PPTP* dapat dilihat pada Tabel 1. Dari hasil uji menjelaskan hasil dari delay adalah 9.276 ms, kemudian data kedua yaitu *jitter* yang bernilai 5.841 ms, data ketiga adalah *throughput* yang bernilai 50% dan data keempat adalah *packet loss* yang bernilai 0%.

Tabel 1 Hasil uji performansi *IAX* tanpa *VPN*

Parameter	**Nilai**
Delay	9.276
Jitter	5.841
Throughput	50%
Packet loss	0%

Hasil uji performansi *VoIP* dengan *protocol IAX* yang menggunakan keamanan *VPN PPTP* dapat dilihat pada Tabel 2. Pada data hasil tersebut menjelaskan hasil dari *delay* adalah 9.580 ms, kemudian data kedua yaitu *jitter* yang bernilai 8.284 ms, data ketiga adalah *throughput* yang bernilai 54% dan data keempat adalah *packet loss* yang bernilai 6.17%.

Tabel 2 Hasil uji performansi *IAX* dengan *VPN*

Parameter	**Nilai**
Delay	9.580
Jitter	8.284
Throughput	54%
Packet loss	6.17%

Hasil uji performansi *VoIP* dengan *protocol SIP* tanpa menggunakan keamanan *VPN PPTP* dapat dilihat pada Tabel 3. Tabel 3. menjelaskan hasil dari delay adalah 9.706 ms, kemudian data kedua yaitu *jitter* yang bernilai 5.541 ms, data ketiga adalah *throughput* yang bernilai 52% dan data keempat adalah *packet loss* yang bernilai 6.17%.

Tabel 3 Hasil uji performansi *SIP* tanpa *VPN*

Parameter	**Nilai**
Delay	9.706
Jitter	5.541
Throughput	52%
Packet loss	6.17%

Hasil uji performansi *VoIP* dengan *protocol SIP* dengan menggunakan keamanan *VPN PPTP* dapat dilihat pada Tabel 4. Tabel 4. menjelaskan hasil dari delay adalah 9.6553 ms, kemudian data kedua yaitu *jitter* yang bernilai 5.101 ms, data ketiga adalah *throughput* yang bernilai 54 % dan data keempat adalah *packet loss* yang bernilai 6 %.

Tabel 4 Hasil uji performansi *SIP* tanpa *VPN*

Parameter	**Nilai**
Delay	9.6553
Jitter	5.101
Throughput	54%
Packet loss	6%

Hasil perbandingan indeks delay dapat dilihat pada Tabel 5. Pengukuran Delay pada *IAX* tanpa *VPN*, *IAX* dengan *VPN*, *SIP* tanpa *VPN* dan *SIP* dengan *VPN* berdasarkan nilai Delay sesuai dengan versi TIPHON sebagai standarisasi, untuk kategori Delay sangat bagus jika < 150 ms, bagus jika 150 ms s/d 300 ms, sedang jika 300 ms s/d 450 ms, dan jelek jika > 450 ms maka didapat Rata – Rata Indeks Delay di Tabel 5 untuk setiap *protocol* adalah "Sangat Bagus" dengan Nilai Indeks "4" dan yang paling kecil delaynya adalah *protocol IAX* tanpa menggunakan keamanan *VPN PPTP*.

Tabel 5 Hasil perbandingan indeks delay

***Protocol* & Keamanan**	**Rata-Rata Delay**	**Rata-Rata**	
		Indeks	**Kategori**
IAX tanpa *VPN*	9.276	4	Sangat bagus
IAX dengan *VPN*	9.580	4	Sangat bagus
SIP tanpa *VPN*	9.706	4	Sangat bagus
SIP dengan *VPN*	9.655	4	Sangat bagus

Hasil perbandingan indeks *jitter* dapat dilihat pada Tabel 6. Pengukuran *Jitter* pada *IAX* tanpa *VPN*, *IAX* dengan *VPN*, *SIP* tanpa *VPN* dan *SIP* dengan *VPN* berdasarkan nilai *Jitter* sesuai dengan versi TIPHON sebagai standarisasi, untuk kategori *Jitter* "Sangat Bagus jika 0 ms,"Bagus" jika 0 ms s/d 75 ms, "Sedang" jika 75 ms s/d 125 ms, dan "Jelek" jika 125 ms s/d 225 ms maka didapat hasil rata-rata indeks *Jitter* di Tabel 6 untuk setiap *protocol* dan keamanan adalah "Bagus" dengan Nilai Indeks "3" dan yang paling rendah *jitter*nya adalah *protocol SIP* dengan menggunakan keamanan *VPN PPTP*.

Tabel 6 Hasil perbandingan indeks *jitter*

***Protocol* & Keamanan**	**Rata-Rata *Jitter***	**Rata-Rata**	
		Indeks	**Kategori**
IAX tanpa *VPN*	5.841	3	Bagus
IAX dengan *VPN*	8.284	3	Bagus
SIP tanpa *VPN*	5.541	3	Bagus
SIP dengan *VPN*	5.101	3	Bagus

Hasil perbandingan indeks *throughput* dapat dilihat pada Tabel 7. Pengukuran *Throughput* pada *IAX* tanpa *VPN*, *IAX* dengan *VPN*, *SIP* tanpa *VPN* dan *SIP* dengan *VPN* berdasarkan nilai *Throughput* sesuai dengan versi TIPHON sebagai standarisasi, untuk kategori *Throughput* sangat bagus jika persentase *Throughput* 100 %, bagus jika persentase *Throughput* 75 %, sedang jika persentase *Throughput* 50 %, dan jelek jika persentase *Throughput* > 25 % maka didapat Rata – Rata Indeks *Throughput* di Tabel 7 untuk setiap *protocol* dan keamanan adalah "Sedang" dengan Nilai Indeks "2" dan yang paling tinggi nilai *throughput*ya adalah *protocol IAX* dan *SIP* dengan menggunakan keamanan *VPN PPTP*.

Hasil perbandingan indeks *packet loss* dapat dilihat pada Tabel 8. Pengukuran *Packet loss* pada *IAX* tanpa *VPN*, *IAX* dengan *VPN*, *SIP* tanpa *VPN* dan *SIP* dengan *VPN* berdasarkan nilai *Packet loss* sesuai dengan versi TIPHON sebagai standarisasi, untuk kategori *Packet loss* "SangatBagus" jika 0 %, "Bagus" jika 3 %, "Sedang" jika 15 %, dan "Jelek" jika 25 % maka didapat Rata – Rata Indeks *Packet loss* di Tabel 8 untuk setiap *protocol* dan keamanan adalah "Bagus" dengan Nilai Indeks "3" dan yang paling rendah *packet loss*nya adalah *protocol IAX* tanpa *VPN*.

Tabel 7 Hasil perbandingan indeks *throughput*

***Protocol* & Keamanan**	**Rata-Rata *Throughput***	**Rata-Rata**	
		Indeks	**Kategori**
IAX tanpa *VPN*	50%	2	Sedang
IAX dengan *VPN*	54%	2	Sedang
SIP tanpa *VPN*	52%	2	Sedang
SIP dengan *VPN*	54%	2	Sedang

Tabel 8 Hasil perbandingan indeks *packet loss*

***Protocol* & Keamanan**	**Rata-Rata *Packet loss***	**Rata-Rata**	
		Indeks	**Kategori**
IAX tanpa *VPN*	0%	4	Sangat Bagus
IAX dengan *VPN*	6.17%	3	Bagus
SIP tanpa *VPN*	6.17%	3	Bagus
SIP dengan *VPN*	6%	3	Bagus

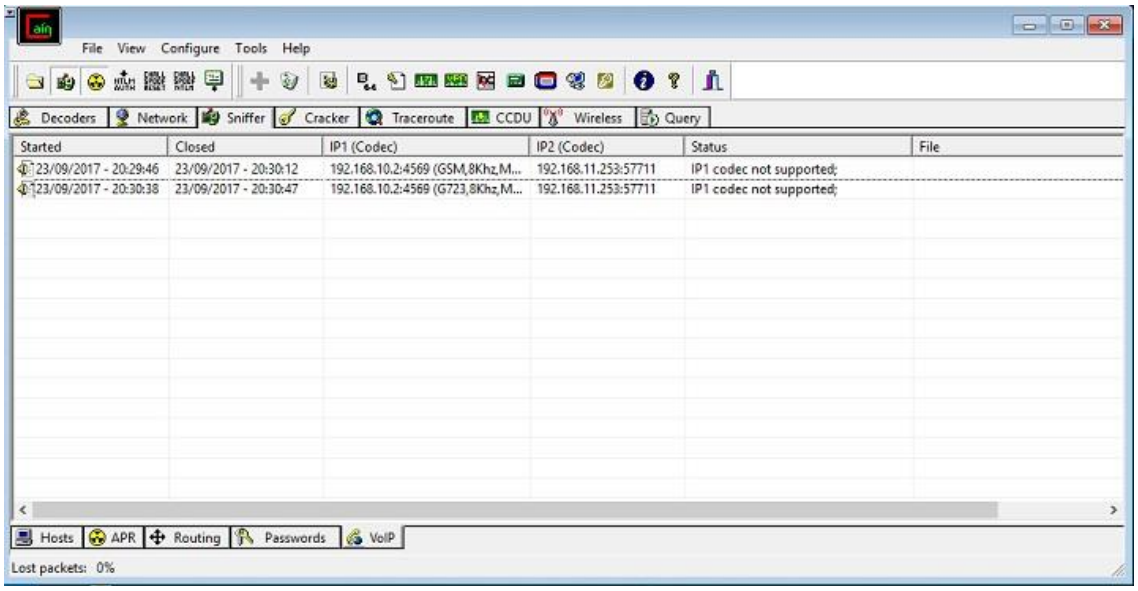
Hasil perbandingan Nilai QoS *VoIP* pada tiap *protocol* dapat dilihat pada Tabel 9. Pengukuran nilai QoS pada tiap *protocol* dengan atau tanpa menggunakan sistem keamanan *VPN* dapat dilihat dari Tabel 9 yaitu hasil akhirnya adalah *protocol IAX* tanpa *VPN*, *IAX* dengan *VPN* dan *SIP* dengan *VPN* adalah memuaskan sedangkan *protocol SIP* tanpa *VPN* hasilnya kurang memuaskan. Tetapi yang paling tinggi nilainya adalah *protocol IAX* tanpa menggunakan sistem keamanan *VPN* yaitu dengan nilai total rata-rata 3.25.

Tabel 9 Hasil perbandingan nilai QoS

Protocol	**Nilai Indeks Delay**	**Nilai Indeks *Jitter***	**Nilai Indeks *Throughput***	**Nilai Indeks *Packet loss***	**Jumlah Rata-Rata Nilai**	**Keterangan Nilai**
IAX tanpa *VPN*	4	3	2	4	3.25	Memuaskan
IAX dengan *VPN*	4	3	2	3	3	Memuaskan
SIP tanpa *VPN*	4	3	2	2	2.75	Kurang Memuaskan
SIP dengan *VPN*	4	3	2	3	3	Memuaskan

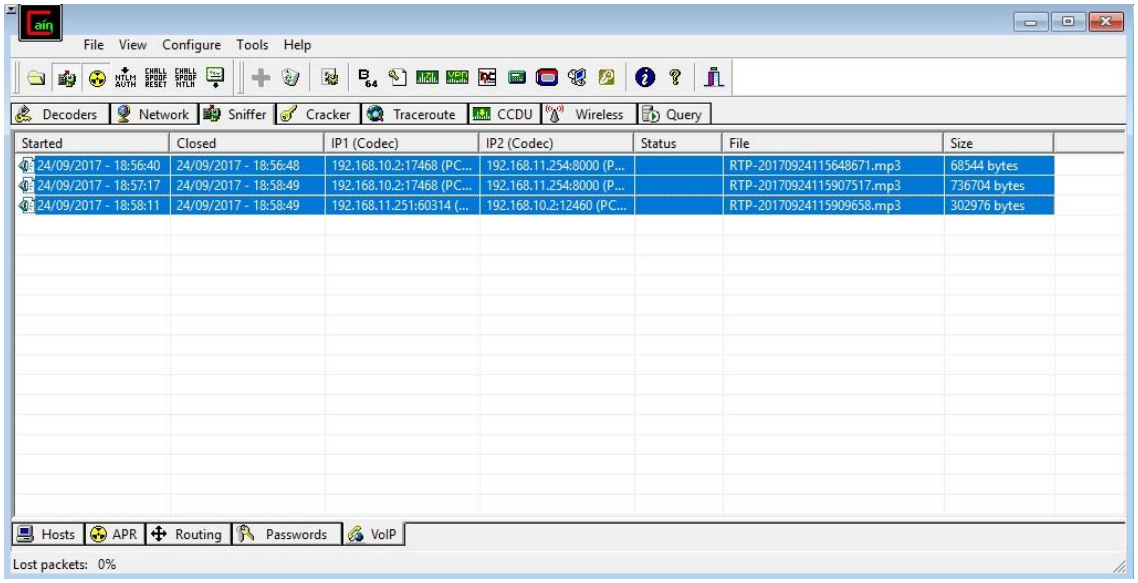
Gambar 4 menjelaskan uji keamanan pada *protocol IAX* tanpa menggunakan keamanan *VPN PPTP* adalah percakapan dari dua *client* dapat disadap menggunakan *software Wireshark* dan hasil sadapan bisa disimpan dan diputar kembali menggunakan *player* yang berarti komunikasi dengan menggunakan *protocol IAX* tanpa mengguanakan keamanan *VPN PPTP* tidak aman dan mempunyai celah untuk penyadapan dari pihak yang tidak bertanggung jawab.

Hasil uji keamanan *VoIP* dengan *protocol IAX* dengan menggunakan keamanan *VPN PPTP* dapat dilihat pada Gambar 5. Pada gambar 5 menjelaskan uji keamanan pada *protocol IAX* dengan menggunakan keamanan *VPN PPTP* adalah percakapan dari dua *client* tidak dapat disadap menggunakan *software Cain and Able* karena pada penelitian ini dihasilkan keterangan bahwa hasil sadapan tidak bisa diputar menggunakan *player* ataupun disimpan dikarenakan paket data percakapan dienkripsi oleh *VPN PPTP* sehingga codec untuk file sadapan tidak bisa dibaca oleh *player* manapun yang berarti komunikasi dengan menggunakan *protocol IAX* dengan mengguanakan keamanan *VPN PPTP* aman dan tidak mempunyai celah untuk penyadapan dari pihak yang tidak bertanggung jawab.

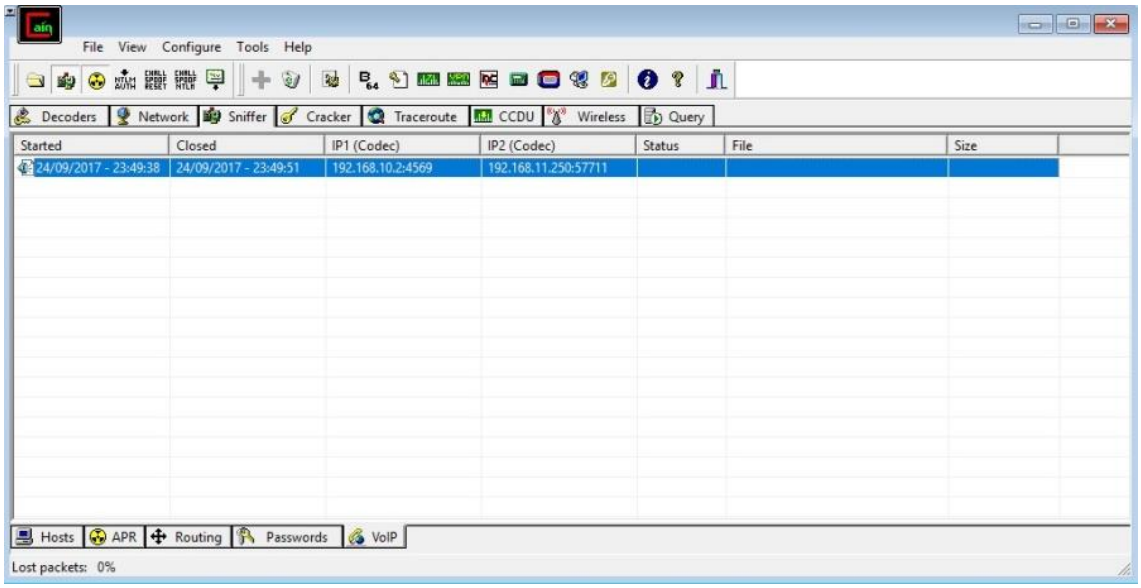


Gambar 4 Hasil uji keamanan *VoIP IAX* dengan *VPN* menggunakan *Cain and Able*

Pada gambar 5 menjelaskan uji keamanan pada *protocol SIP* tanpa menggunakan keamanan *VPN PPTP* adalah percakapan dari dua *client* dapat disadap menggunakan *software Cain and Able* dan hasil sadapan bisa disimpan dan diputar kembali menggunakan *player* yang berarti komunikasi dengan menggunakan *protocol SIP* tanpa mengguanakan keamanan *VPN PPTP* tidak aman dan mempunyai celah untuk penyadapan dari pihak yang tidak bertanggung jawab. Pada gambar 6 menjelaskan uji keamanan pada *protocol SIP* dengan menggunakan keamanan *VPN PPTP* adalah percakapan dari dua *client* tidak dapat disadap menggunakan *software Cain and Able* karena pada penelitian ini dihasilkan keterangan bahwa hasil sadapan tidak bisa diputar menggunakan *player* ataupun disimpan dikarenakan paket data percakapan dienkripsi oleh *VPN PPTP* sehingga codec untuk file sadapan tidak bisa dibaca oleh *player* manapun yang berarti komunikasi dengan menggunakan *protocol SIP* dengan mengguanakan keamanan *VPN PPTP* aman dan tidak mempunyai celah untuk penyadapan dari pihak yang tidak bertanggung jawab.



Gambar 5 Hasil uji keamanan *VoIP SIP* tanpa *VPN* menggunakan *Cain and Able*



Gambar 6 Hasil uji keamanan *VoIP SIP* dengan *VPN* menggunakan *Cain and Able*

4. KESIMPULAN DAN SARAN

Pada uji performansi *delay, jitter, throughput dan packet loss* pada tiap *protocol VoIP* dengan atau tanpa menggunakan sistem keamanan *VPN* yang paling tinggi nilainya adalah *protocol IAX* tanpa menggunakan sistem keamanan *VPN* yaitu dengan nilai rata-rata 3.25 mendekati predikat sangat memuaskan. Pada uji tingkat keamanan tiap *protocol VoIP* dengan atau tanpa menggunakan sistem keamanan *VPN* dapat dilihat hasilnya tiap *protocol* yang menggunakan sistem keamanan *VPN* lebih aman daripada *protocol VoIP* yang tidak menggunakan sistem keamanan *VPN* dikarenakan *protocol* yang menggunakan *VPN* tidak terbaca pada saat penyadapan dilakukan pada *software sniffing* atau penyadap dikarenakan paket data yang dikirim maupun yang diterima antar *client* dienkripsi oleh sistem *VPN PPTP*

pada *server VPN router*.

Pada kasus pekerjaan ini, dapat disimpulkan *protocol* yang sesuai digunakan untuk membangun sistem komunikasi *VoIP* adalah "*Protocol IAX* " dikarenakan nilai QoSnya lebih tinggi daripada *protocol SIP* dan juga terbukti saat diterapkan sistem keamanan *VPN software* penyadap tidak dapat membaca paket data percakapan dikarenakan telah dienkripsi oleh sistem *VPN PPTP*.

Penelitian selanjutnya bisa ditujukan pada pengembangan jaringan *VoIP* terintegrasi pada teknologi *Internet of Things*, seperti diketahui bahwa koenktifitas jaringan komputer dan telekomunikasi di era revolusi industri ini menjadi kunci utama untuk kepentingan analisis yang lebih luas. Pengujian dan analisis tingkat keamanan pada *embedded system over VoIP Intertet of Things* menjadi tantangan pekerjaan penelitian yang menarik untuk dikerjakan selanjutnya.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Jurusan Teknik Elektro atas dukungan dan fasilitas Laboratorium Elektronika dan Jaringan Komputer yang disediakan guna terlaksananya pekerjaan ini. Kepada Fakultas Teknik, Universitas Muhammadiyah Malang, atas dukungan melalui skema program Penelitian dan Pengabdian Fakultas PUSKAREKA, terima kasih dan apresiasi diberikan yang setinggi-tingginya.

DAFTAR PUSTAKA

[1] L. S. Tanutama, R. A. Poernama, Yansen, and W. Riani, "Performansi Komunikasi VoIP – SIP Dengan GSM Melalui GSM Gateway," *J. Tek. Komput.*, vol. 18, no. 2, pp. 100–108, 2008.

[2] Y. Patih, D. F. J., Fitriawan, H., & Yuniati, "Analisa Perancangan Server Voip (Voice Internet Protocol) Dengan Opensource Asterisk Dan VPN (Virtual Private Network) Sebagai Pengaman Jaringan Antar Client," *J. Inform. Dan Tek. Elektro Terap.*, vol. 1, no. 1, pp. 42–48, 2012.

[3] E. B. Setiawan, "Analisa Quality Of Services (QoS) Voice Over Internet Protocol (VoIP) Dengan Protokol H.323 Dan Session Initial Protocol (SIP)," *J. Ilm. Komput. Dan Inform.*, vol. 1, no. 2, pp. 1–8, 2012.

[4] M. I. Wahyuddin, "Implementasi Voip Computer To Computer Berbasis Freeware Menggunakan Session Initiation Protocol," *J. Artif. ICT Res. Cent.*, vol. 3, no. 1, pp. 50–59, 2009.

[5] N. Yuliana, M., Kristalina, P., & Munif, "Analisa dan Implementasi VoIP SIP pada Mobile Phone di Jaringan Bluetooth," *EEPIS J.*, pp. 73–81, 2010.

[6] B. Prasetyo, "Analisis Implementasi Voice Over Internet Protocol (VoIP) Pada Jaringan Wireless LAN Berbasis Session Initiation Protocol (SIP)," Telkom University, 2006.

[7] Ç. Yıldız, B. Kurt, T. Y. Ceritli, B. Sankur, and A. T. Cemgil, "A real-time SIP network simulation and monitoring system," *SoftwareX*, vol. 8, pp. 21–25, 2018.

[8] E. Mufida, D. Irawan, and G. Chrisnawati, "Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus Pada Yayasan Teratai Global Jakarta," *J. MATRIK*, vol. 16, no. 2, pp. 9–19, 2017.

[9] W. Bin Hsieh and J. S. Leu, "Implementing a secure VoIP communication over SIP-based networks," *Wirel. Networks*, vol. 24, no. 8, pp. 2915–2926, 2018.

[10] M. I. Haji, S. Purwantoro, and S. P. Arifin, "Analysis Tunneling IPv4 and IPv6 on VoIP Network," *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 3, no. 4, pp. 337–344, 2018.

[11] I. W. E. P. Darmawan, "Rancang Bangun Keamanan Transfer Data Voip Over Vpn Pada Sistem Opensource Trixbox," *J. Pendidik. Teknol. dan Kejuru.*, vol. 11, no. 1, pp. 1–12,

2014.

[12] P. K. Dhillon and S. Kalra, "Secure and efficient ECC based SIP authentication scheme for VoIP communications in internet of things," *Multimed. Tools Appl.*, pp. 22199–22222, 2019.

[13] D. A. Wijaksono, "Pembuatan Jaringan PABX Dengan Sistem VoIP Menggunakan Sistem Operasi Linux Trixbox," Universitas Muhammadiyah Surakarta, 2012.

[14] F. Z. Nasihin, A. B. P. Negara, and A. Irwansyah, "Studi Perbandingan Performa QoS (Quality of Service) Tunneling Protocol PPTP Dan L2TP Pada Jaringan VPN Menggunakan Mikrotik," *J. Sist. dan Teknol. Inf.*, vol. 4, no. 1, pp. 1–6, 2016.