

Analisis Performansi Video Conference Menggunakan Codec H264 Baseline dan H264-High Profile dengan Enkripsi Terintegrasi

Mohammad Fazrie

Teknik Elektro, Universitas Mercu Buana, Jakarta
Mo.fazrie@gmail.com

Abstrak

Jumlah penggunaan video conference di dunia semakin berkembang, dengan tingginya penggunaan video conference semakin tinggi pula aspek-aspek yang diperhatikan, diantaranya aspek kenyamanan dan keamanan. Berbicara tentang aspek kenyamanan pada video conference tidak lepas dari kompresi yang digunakan, baik kompresi audio dan video. Dewasa ini teknologi kompresi untuk video sudah sampai pada codec H.264 dan H.264-High Profile, dengan menggunakan teknologi H.264-High Profile dapat mengkonsumsi bandwidth setengah dari H.264 (tanpa enkripsi). Berbicara aspek keamanan tidak lepas dari enkripsi lalu lintas data termasuk audio dan video yang dapat di enkripsi. Untuk itulah agar dapat mendekati aspek keamanan dan kenyamanan yang seimbang perlu di analisa dan di teliti mengenai performa H.264 dan H.264-High Profile yang telah di enkripsi. Untuk meneliti tingkat aspek performa dan keamanan video conference perlu adanya teknik dan metode yang di gunakan. Dengan memanfaatkan parameter jitter , packet loss , dan PSNR kita dapat menarik kesimpulan baik atau tidaknya performa video conference. Namun untuk aspek keamanan, percakapan dua arah atau lebih harus dipastikan agar tidak dapat dilihat dan kompatibel dengan perangkat video conference yang ada. Dengan memanfaatkan teknik enkripsi pada layer 2 atau 3 hal ini memungkinkan dapat dilakukan.

Keyword : Enkripsi, H.264, H264-HP, Video conference

Received September 2016

Accepted for Publication January 2017

1. PENDAHULUAN

Penggunaan video conference dewasa ini kian berkembang hampir diseluruh Negara di dunia tidak terkecuali di Indonesia. Pemanfaatan video conference digunakan pada berbagai institusi, diantaranya pemerintahan, pendidikan, perbankan dan industri. Karena video conference digunakan sebagai media komunikasi antara dua arah atau lebih, maka perlu adanya aspek kenyamanan dan keamanan.

Dengan melihat market Video conference yang cukup besar tidak sedikit vendor teknologi telekomunikasi ikut serta dalam mengembangkan aspek bisnis dan teknologi video conference. Dengan begitu, meskipun sudah adanya badan standarisasi Internasional (ITU-T) terkait teknologi video conference. Vendor-vendor mencoba untuk mengembangkan, menambahkan, dan berinovasi terkait produk masing-masing untuk menunjukkan kelebihan masing-masing produk. Beberapa hal yang signifikan dikembangkan dalam teknologi video conference yaitu aspek keamanan, kompresi, dan fitur untuk dapat saling terintegrasi. Namun dengan adanya persaingan inovasi dalam teknologi tersebut tidak semua fitur dapat saling terintegrasi secara utuh.

Berbicara mengenai video conference tidak lepas dari teknologi video coding (Codec) yang digunakan, saat ini video coding yang digunakan dan menjadi rekomendasi oleh ITU-T yaitu H.264. Berbagai vendor berlomba-lomba untuk melakukan inovasi yang memungkinkan codec H.264 dapat dikembangkan menjadi sebuah kompresi video yang lebih kecil dalam mengkonsumsi bandwidth, muncullah pengembangan teknologi codec tersebut yang dikenal dengan H.264-HP (High Profile). Teknologi High Profile memungkinkan mendapatkan resolusi yang sama dengan H.264 dengan call rate 50% lebih kecil dari H.264.

Namun kenyamanan yang diberikan dari suatu teknologi sangat perlu memperhatikan aspek keamanan agar porsi keseimbangan antara kenyamanan dan keamanan dapat seimbang. Salah satu teknik pengamanan telekomunikasi dari penyadapan (eavesdropping) yaitu dengan cara mengenkripsi jalur data end to end. Dapat dibayangkan jika pada saat komunikasi menggunakan teknologi videoconference pada suatu perusahaan membahas hal yang bersifat rahasia namun paket data dapat dilihat, dapat di sadap (eavesdropping) direkam dan di playback.

Teknik dalam melakukan enkripsi terdapat berbagai cara dalam mengimplementasikannya. Enkripsi dapat dilakukan pada layer 2,3 dan 7 penggunaan enkripsi pada setiap layer ditentukan oleh kondisi topology jaringan, penggunaan perangkat itu sendiri, dan tujuan pengamanan.

Tujuan penelitian ini dilakukan, untuk mendapatkan suatu hasil dimana mekanisme enkripsi pada video conference dapat kompatibel dengan berbagai macam brand juga mendapatkan nilai dari penghitungan performa video coding (codec) H.264 H.264-HP jika dienkripsi. Sasaran penelitian ini dilakukan yaitu untuk, mendapatkan metode yang tepat, untuk melakukan enkripsi agar paket video conference tidak terlihat (terenkripsi) dan kompatibel dan mengetahui secara statistic hasil performa video coding (codec) H.264 dan H.264-HP jika terenkripsi.

2. KAJIAN PUSTAKA

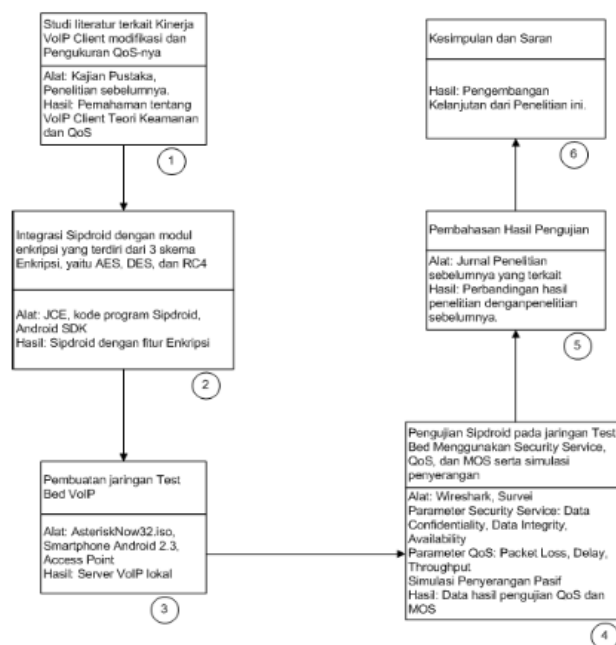
Di bagian ini dibahas dan dikaji beberapa penelitian terkait yang pernah dilakukan sebelumnya. Adapun pemaparan yang akan disajikan meliputi beberapa penelitian mengenai performa video, codec H.264 dan enkripsi:

Wahab a. , Bahaweres, R.B, Alaydrus, M., Muhaemin, M., Sarno, R.,(2012) dalam penelitiannya yang berjudul "Performance analysis of VoIP client with integrated encryption module" [1].

Kesimpulan pada penelitian ini adalah sebagai berikut :

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

Gambar 1 menunjukkan metoda penelitian yang digunakan di penelitian [1].



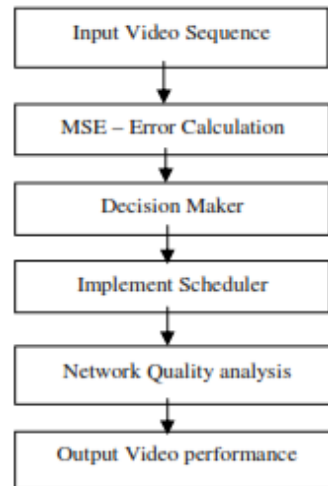
Gambar 1 Metode penelitian dari publikasi [1] Performance analysis of VoIP client with integrated encryption module

Barath S., Jaganath S., Prakash J. (2013) dalam penelitiannya yang berjudul “Perceptual Video Quality Measurement Based on Generalized Priority Model” [2], dengan metoda yang ditampilkan di gambar 2.

Dalam tulisannya, diusulkan suatu model linier umum untuk meminimalkan degradasi kualitas visual. Kemudian manfaat dan kontribusi dari hasil penelitian tersebut yaitu :

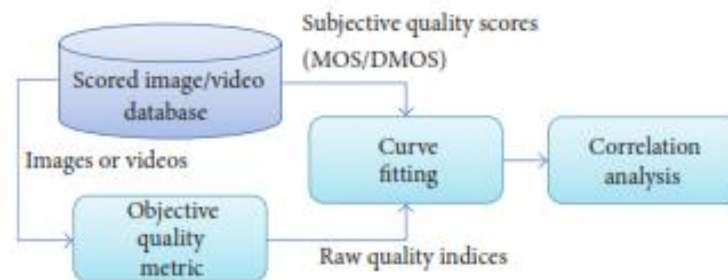
- 1) Tidak seperti model sebelumnya, model visibilitas ini dikembangkan pada dataset dari beberapa percobaan subjektif menggunakan codec yang berbeda, pengaturan encoder yang berbeda, dan berbeda strategi penyembunyian error decoder. Jadi model memiliki penerapan yang luas.

- 2) Penulis menggunakan model visibilitas untuk memprioritaskan paket video dan merancang kebijakan untuk berbasis persepsi kualitas paket. Meskipun model dirancang untuk video berkualitas tinggi yang diangkut melalui kualitas jaringan yang baik, percobaan menunjukkan bahwa Model berkerja dengan baik untuk video dengan berbagai tingkat encoding.
- 3) Analisis pada paket tingkat kesalahan menunjukkan bahwa model yang telah penulis uji. Hal ini menunjukkan bahwa evaluasi kualitas video hanya didasarkan pada tingkat packet loss yang tidak akurat.



Gambar 2 Block Diagram Generalized Linear Models (GLM)

Martínez-Rach Miguel O., Pablo Piñol, López Otoniel M., Malumbres Manuel Perez, Oliver José, dan Calafate Carlos Tavares (2014) dalam penelitiannya yang berjudul “On the Performance of Video Quality Assessment Metrics under Different Compression and Packet Loss Scenarios” [3], dengan metoda pendekatan Quality Assessment Matrix (QAM) yang ditunjukkan di gambar 3.



Gambar 3 Block Diagram QAM (Quality Assessment Matrix)

Tabel 1 menampilkan perbandingan penelitian terdahulu dengan penelitian yang dilakukan di sini.

Tabel 1 Studi Penelitian terdahulu dan perbandingannya dengan penelitian ini

Peneliti	Ruang Lingkup Pembahasan	Topik
Wahab a. , Bahaweres, R.B, Alaydrus M., Muhaemin, M., Sarno, R. (2012) [1]	VoIP, VoIP Client, Encryption	<i>Performance analysis of VoIP client with integrated encryption module</i>
Barath S., Jaganath S., Prakash J. (2013) [2]	Packet dropping policy; packet loss; perceptual video quality; video coding; visibility model	<i>Perceptual Video Quality Measurement Based on Generalized Priority Model</i>
Martínez-Rach Miguel O., Pablo Piñol, López Otoniel M., Malumbres Manuel Perez, Oliver José, dan Calafate Carlos Tavares (2014) [3]	Performance Video, QAM , Compression, Packet Loss	<i>On the Performance of Video Quality Assessment Metrics under Different Compression and Packet Loss Scenarios</i>
Gu Meihua., Yu Ningmei, Kou Likang., dan Jiang Chang, (2010) [4]	H.264/AVC; Mode Decision; Temporal Homogeneity; Spatial Homogeneity; Texture Direction	<i>Hybrid Fast Mode Decision Algorithm for H.264/AVC High Profile</i>
Ibrahim Mohamed M., Kader Neamat S. Abdel, dan Zorkany M. (2014) [5]	Watermarking Technic, Interlacing, DWT	<i>Video Multiple Watermarking Technique Based on Image Interlacing Using DWT</i>

3. METODE PENELITIAN

3.1. Teknik Analisis

Dalam menganalisa performansi sistim digunakan besaran-besaran kuantitatif seperti rasio sinyal puncak terhadap noise (Peak Signal Noise Ratio /PSNR), Variasi waktu tunda (Variation of delay atau jitter), dan paket yang hilang (Packet Loss).

3.1.1 Peak Signal Noise Ratio (PSNR)

PSNR sering dinyatakan dalam skala logaritmik dalam decibel (dB). Nilai PSNR jatuh dibawah 30 dB mengindikasikan kualitas yang relative rendah, dimana distorsi yang dikarenakan penyisipan terlihat jelas. Akan tetapi kualitas stego-image yang tinggi berada pada nilai 40dB dan diatasnya [6] dan menurut ITU standar threshold minimal berada pada 20dB. PSNR didefinisikan pada persamaan berikut

$$\begin{aligned} PSNR &= 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \\ &= 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right) \end{aligned} \quad (1)$$

Dimana MSE dinyatakan sebagai mean square error yang didefinisikan sebagai berikut

$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - K(i, j)]^2 \quad (2)$$

3.1.2 Variasi Waktu Tunda (Jitter)

Variasi waktu tunda (jitter) merupakan perbedaan selang waktu kedatangan antar paket di terminal tujuan. Variasi waktu tunda dapat disebabkan oleh terjadinya kongesti, kurangnya kapasitas jaringan, variasi ukuran paket, serta ketidakteraturan paket. Tabel 2 memberikan korespondensi besaran kuantitatif dari jitter dalam satuan milisekon dengan kualitas.

Tabel 2 Standar nilai variasi waktu tunda berdasarkan ITU G.114

Variasi waktu tunda (ms)	Kualitas
0 – 20	Baik
20 – 50	Dapat diterima
> 50	Tidak dapat diterima

3.1.3 Paket yang hilang (Packet Loss)

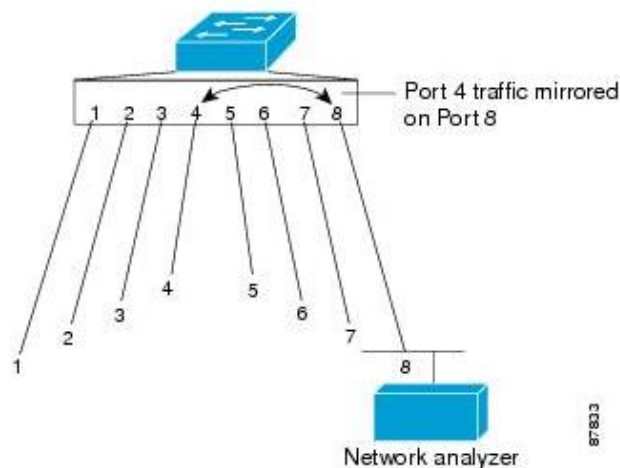
Paket hilang (packet loss) merupakan penyebab utama pelemahan audio dan video pada multimedia streaming. Paket hilang dapat disebabkan oleh pembuangan paket di jaringan (network loss) atau pembuangan paket di gateway/terminal sampai kedatangan terakhir (late loss). Tabel 3 menunjukkan rekomendasi nilai paket hilang yang mempengaruhi kualitas layanan (QoS) atau performa video.

Tabel 3 Rekomendasi nilai paket hilang berdasarkan ITU G.114

Paket Hilang (%)	Kualitas
0 – 1	Baik
1 – 5	Dapat diterima
> 10	Tidak dapat diterima

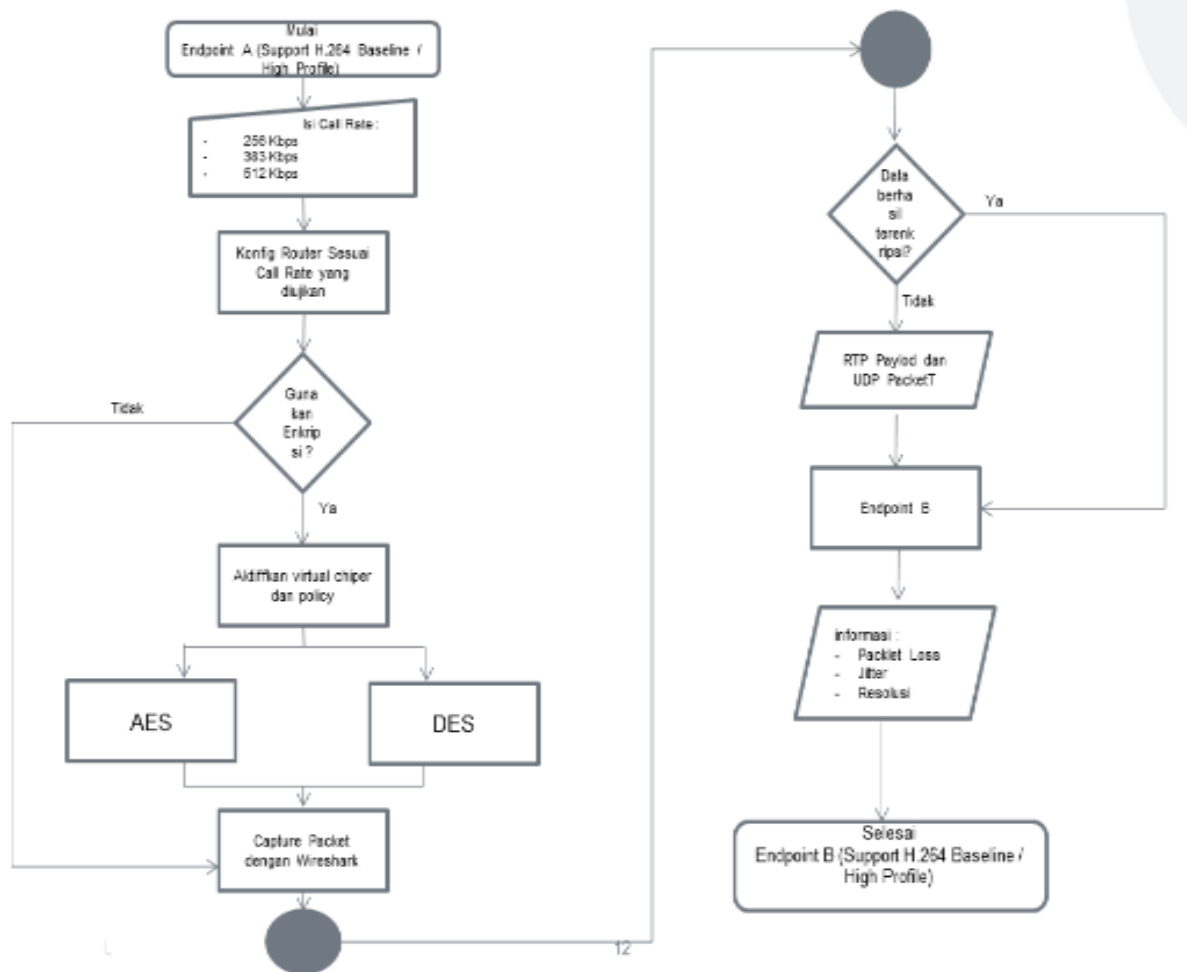
3.2. Metode Pengumpulan Data dengan Switched Port Analyzer

Port mirroring adalah fitur dimana trafik data pada suatu port ataupun vlan pada sebuah switch bisa di tampilkan di port yang lain, baik itu pada switch yang sama maupun berbeda VLAN. Di penelitian ini teknik tersebut dimanfaatkan untuk membaca paket video yang lewat. Gambar 4 menampilkan konsep pengukuran dengan menggunakan Switched Port Analyzer (SPAN).



Gambar 4 SPAN Konsep dan Terminologi

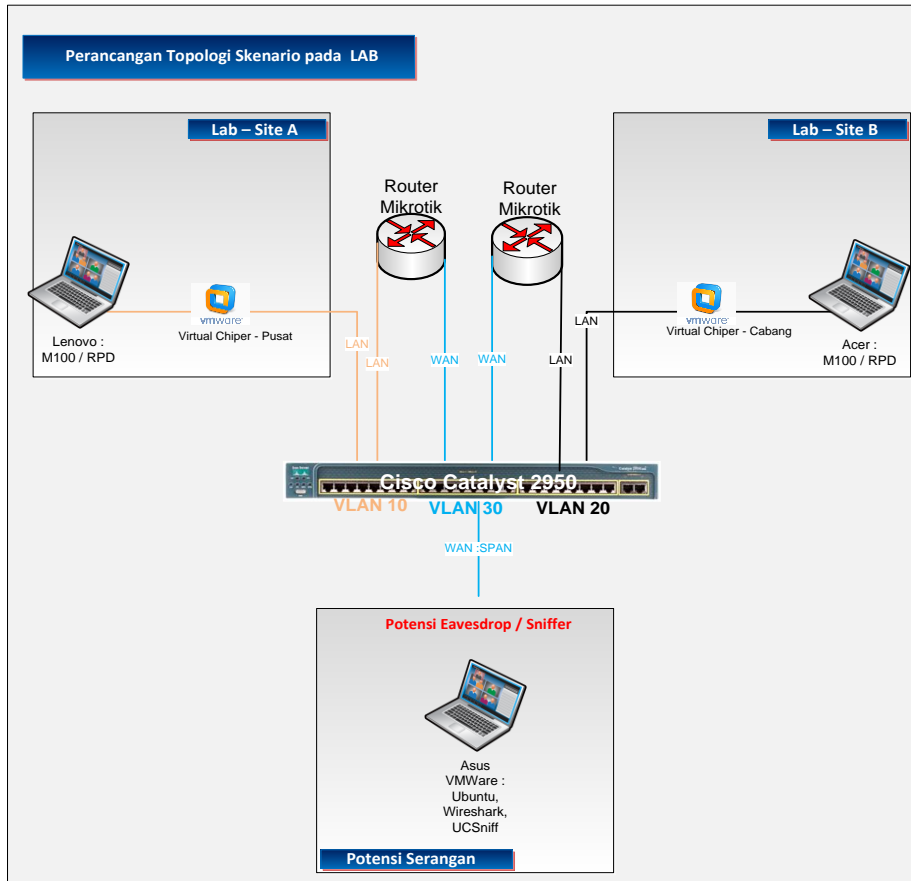
Metoda penelitian yang digunakan di sini ditampilkan di gambar 5. Dua enkripsi yang bisa dipilih AES dan DES.



Gambar 5 Diagram alir perancangan proses penelitian

Panggilan video yang dilakukan bisa menggunakan 256 kbps, 383 kbps atau 512 kbps. Dengan menggunakan software Wireshark, data trafik bisa diobservasi dan bisa didapatkan informasi tentang packet loss, jitter dan resolusi.

Gambar 6 menampilkan testbed yang digunakan untuk melakukan penelitian dan pengumpulan data kuantitatif.



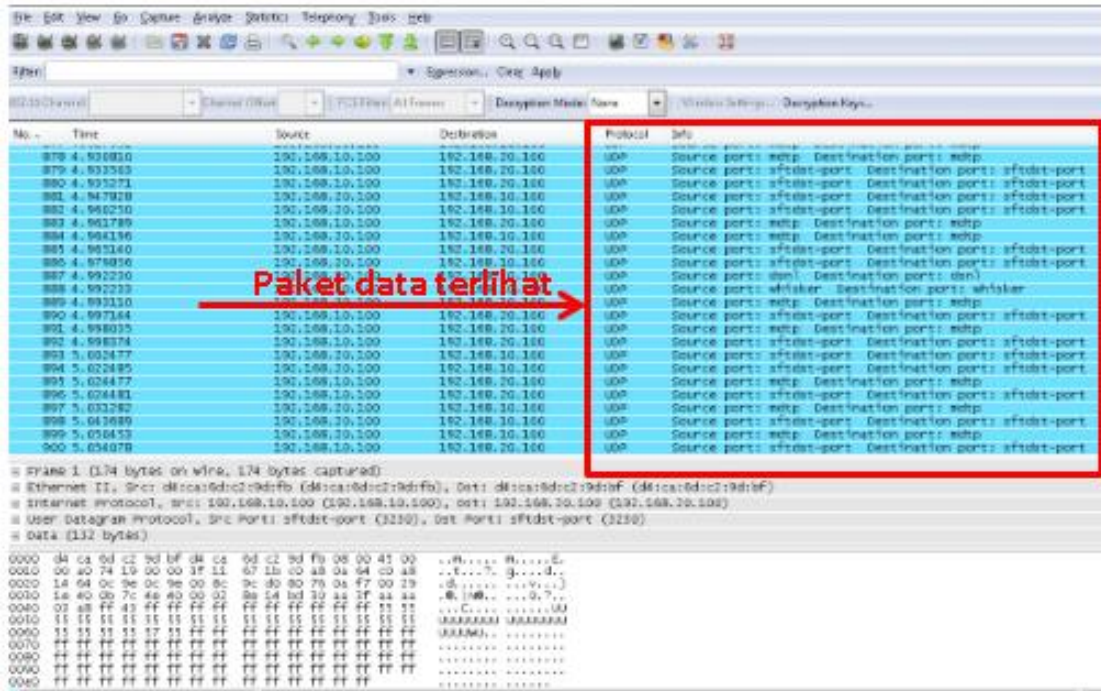
Gambar 6 Perancangan topologi scenario.

4. HASIL DAN ANALISIS

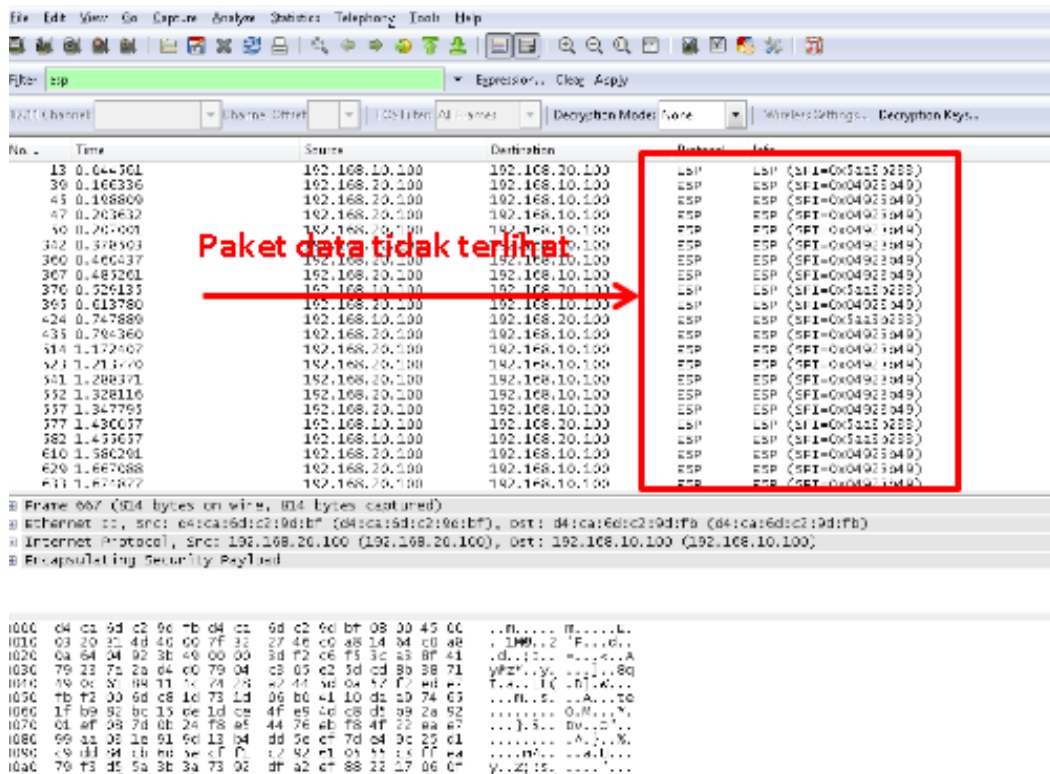
Pada data dan sampel yang diujikan terdiri dari beberapa call rate yang diujikan diantaranya 256 Kbps, 384 Kbps, dan 512 Kbps. Dan untuk codec yang diujikan yaitu H.264 Baseline dan H.264 High Profile, kemudian enkripsi yang digunakan yaitu AES dan 3DES. Hasil ini dianalisis dengan parameter PSNR dan penghitungan table jitter dan paket loss.

4.1. Hasil Enkripsi Paket Data Video Conference

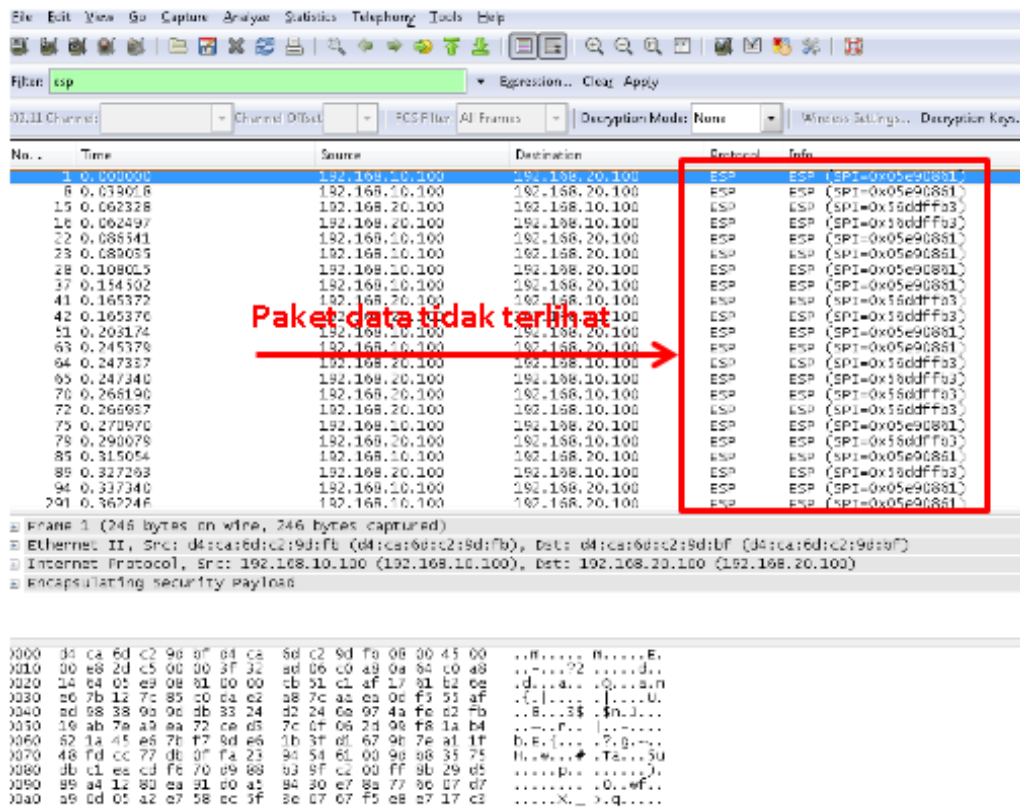
Pada bagian ini dilakukan penelitian dengan menggunakan aplikasi monitoring dengan meng-capture packet yang lewat dengan teknik SPAN, dan mencoba untuk membandingkan bagaimana paket yang tidak terenkripsi dan paket yang telah terenkripsi. Hasil capture tersebut menjadi dasar dari pengamatan lanjutan. Gambar 7 menunjukkan hasil sesi panggilan tanpa enkripsi, sedangkan gambar 8 dan 9 masing-masing untuk enkripsi 3DES dan AES.



Gambar 7 Hasil capture pada session call tanpa enkripsi.



Gambar 8 Hasil capture pada session call dengan enkripsi 3DES.



Gambar 9 Hasil capture pada session call dengan enkripsi AES.

Dari hasil capture paket di gambar-gambar 7,8 dan 9 ini, dapat dilihat bahwa pada saat session call tidak terenkripsi, table protocol dan info dapat dilihat namun pada saat dienkripsi tabel protocol dan info dapat dilihat, potensi untuk melakukan eavedropping dapat menjadi lebih besar dengan memanfaatkan informasi yang terbaca dari capture packet source dan destination paket tersebut.

4.2. Analisa Packet Loss dan Jitter

Di bagian ini diamati hasil dengan codec H.264 baseline call rate 256 kbps (tabel 4) dan high profile call rate 256 kbps (tabel 5). Pada dua opsi ini didapatkan packet loss yang sangat kecil < 1% sehingga bisa dikatakan terkait packet loss, sistim berkualitas baik. Jitter yang diamati pada baseline call membesar dengan digunakannya enkripsi, yaitu dari 23 ms tanpa enkripsi menjadi masing-masing 28 ms dan 30 ms untuk 3DES dan AES. Semua nilai ini masih masuk kategori kualitas dapat diterima.

Tabel 4 Analisa Codec H.264 Baseline call rate 256 Kbps

256 Kbps	Tidak Di enkripsi	Enkripsi 3 DES	Enkripsi AES
Paket loss	0%	0%	0%
Jitter	Tx: 23 Rx: 3	Tx: 28 Rx: 5	Tx: 30 Rx: 6
Resolusi	Tx: 640x360 Rx: QVGA	Tx: 640x360 Rx: QVGA	Tx: 640x360 Rx: QVGA

Sedangkan jitter pada opsi high profile call rate 256 kbps, justru didapatkan jitter yang sedikit mengecil dari 22 ms ke 20 ms.

Tabel 5 Analisa Codec H.264 High Profile call rate 256 Kbps

256 Kbps	Tidak Di enkripsi	Enkripsi 3 DES	Enkripsi AES
Paket loss	0%	0%	0%
Jitter	Tx: 22 Rx: 1	Tx: 20 Rx: 22	Tx: 20 Rx: 29
Resolusi	Tx: 640x360 Rx: 640x360	Tx: 640x360 Rx: 640x360	Tx: 640x360 Rx: 640x360

4.3. Analisa PSNR

Penghitungan PSNR pengujian berdasarkan hasil call rate yang telah diujikan kemudian dari data yang didapat dimasukkan ke dalam persamaan PSNR berikut adalah persamaan (2) dan (1).

Secara umum data yang didapatkan dari pengukuran menunjukkan enkripsi dengan 3DES atau AES tidak menurunkan nilai PSNR secara signifikan, karena nilai PSNR semua lebih besar dari 20 dB, sebagai besaran minimal yang ditetapkan oleh ITU.

Tabel 6 Penghitungan PSNR Codec H264 High Profile Enkripsi 3DES

Call Rate	Rate $t_x(M)$	Rate $r_x(N)$	Resolusi	MSE	PSNR
256 Kbps	190	199	640x360	0.0003	31.7 db
384 Kbps	318	313	640x360	0.0001	56 db
512 Kbps	427	378	640x360	0.01	36 db

Tabel 7 Penghitungan PSNR Codec H264 High Profile Enkripsi AES

Call Rate	Rate $t_x(M)$	Rate $r_x(N)$	Resolusi	MSE	PSNR
256 Kbps	185	195	640x360	0.0004	30 db
384 Kbps	331	301	640x360	0.0001	36 db
512 Kbps	428	357	640x360	0.0036	41 db

5. KESIMPULAN

Tujuan penelitian ini yaitu menganalisa performa video conference dengan membandingkan kedua codec yaitu H.264 Baseline dan H.264 High Profile, dengan kondisi enkripsi yang terintegrasi tidak pada layer 7 (aplikasi), dengan adanya enkripsi di layer 2 atau 3 hal ini memungkinkan video conference dapat saling komunikasi walaupun berbeda teknologi dan brand namun tetap terenkrip.

Dari hasil penelitian penulis mengambil kesimpulan, bahwa codec H.264 High Profile lebih baik dibandingkan dengan H.264 Baseline dalam mengkompresi video hal ini dibuktikan dari resolusi yang didapatkan lebih tinggi yaitu sebesar 640x360 pada callrate 512 Kbps sedangkan H.264 Baseline 640x240. Kemudian dari aspek keamanan enkripsi AES lebih berat dibanding dengan 3DES, hal ini dibuktikan adanya paket loss pada enkripsi AES sebesar 1%. Kemudian dari sisi PSNR decibel terendah ada pada codec H.264 Baseline yang telah terenkripsi AES yaitu sebesar 25 db. Namun dari hasil keseluruhan penelitian kualitas video dapat dikatakan baik walaupun terintegasi dengan enkripsi.

REFERENCES

- [1] A Wahab, RB Bahaweres, M Alaydrus and R Sarno. "Performance analysis of VoIP client with integrated encryption module". 2013 1st Int. Conf. Commun. Signal Process. their Appl. 2013: 1–6.
- [2] S. Bharath, S. Jaganath, J. Prakash, Perceptual Video Quality Measurement Based on Generalized Priority Model, International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 2, Issue. 4, April 2013, pp. 58 – 64.
- [3] Miguel O., Pinol M., Lopez M., & Malumbers P. (2014). " On the Performance of Video Quality Assesment Metric under Different Compression and Packet Loss Scenario" The Scientific World Journal, Vol. 2014, Article ID 743604.
- [4] Meihua Gu, Ningmei Yu, Likang Kou, Chang Jiang, Hybrid Fast Mode Decision Algorithm for H.264/AVC High Profile, Journal of Information & Computational Science 7: 10 (2010) 2071–2079.
- [5] Mohamed M. Ibrahim, Naemat S. Abdul Kader, & M. Zorkany (2014) "Video Multiple Watermarking Technique Based on Image Interlacing Using DWT", The Scientific World Journal, Hindawi, 2014, Article ID 634828.
- [6] Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKeivitt, "A hash-based image encryption algorithm", Optics Communications, Volume 283, Issue 6, 15 March 2010, Pages 879–893.
- [7] Bryan Yonathan, Yoanes Banding, & Armein Z.R Lang (2011) "Analisis Kualitas Layanan (QoS) Audio-Video Layanan Kelas Virtual Di Jaringan Digital Learning Pedesaan" Konferensi Teknologi Informasi dan omunikasi untuk Indonesia, e-initiative 2011.
- [8] CISCO Inc. http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2940/software/release/12-1_19_ea1/configuration/guide/2940scg_1/swspan.html?referring_site=RE&pos=1&page=http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41.html
- [9] Gu Meihua, Yu Ningmei, Kou Likang, & Jiang Chang (2015) "Image Encryption Algorithm Based on Chaotic Economic Model", Mathematical Problem in Engineering, 2015, Article ID 341729.
- [10] Ian E. G. Rrichardson "H.264 and MPEG-4 Video Compression: Video Coding for Next Generation Multimedia" The Robert Gordon University, Aberdeen.

- [11] Ira M. Weinstein & Andy Nilsen Winhouse Research (2013) "End Survey: The Real Benefit of Video"
- [12] ITU-T H.264(2011) "Series H: Advanced Video Coding for Generic Audiovisual Services" AUDIOVISUAL AND MULTIMEDIA SYSTEMS, Recommendation ITU-T H.264.
- [13] Robert F. Mason and Tom Eagle (2013) "Marketscope for Group Video System" GARTNER, ID: G00252806
- [14] Robert R. (2009) "Video Conferencing in Distance Learning: A New Zealand Schools Perspective" Journal of Distance Learning, 2009, 13(1), 91-107. UK. ISBN 0-470-84837-5
- [15] Winhouse Research (2010) "WR Investigates Polycoms Claim of No-Compromise Performance Using up to 50% Less Bandwidth", Evaluation: Polycom Implementation of H.264 High Profile"