Analisa Pengaruh Routing Protokol Dan Mekanisme Keamanan Pada Kualitas Layanan Multimedia pada Jaringan IP

I Made Suartana[1], Henni Endah Wahanani[2], Aditia Mieka Darminta[3]

[1] Teknik Informatika, Universitas Negeri Surabaya
[2,3]Teknik Informatika, Universitas Pembangunan Nasional "Veteran" Jatim
[1]madesuartana@unesa.ac.id
[2]henniendah222@gmail.com
[3]adityamieka@gmail.com

***Abstrak*— Layanan multimedia melalui jaringan internet seperti, teknologi Voice over IP (VoIP), video on-demand (VoD), IP television (IPTV), konferensi video beresolusi tinggi dan beberapa aplikasi real time, akhir-akhir ini trafiknya terus meningkat. Layanan multimedia memiliki persyaratan QoS yang tinggi terhadap *loss*, *delay*, *jitter*, dll. Ada banyak faktor yang menyebabkan penurunan kualitas layanan multimedia pada jaringan seperti penggunaan protokol routing dan termasuk juga mekanisme keamanan yang digunakan pada jaringan. Memiliki sistem komunikasi yang aman itu penting, baik untuk urusan bisnis atau pribadi, tetapi penting juga untuk menjaga kinerja dari layanan karena mekanisme keamanan memiliki efek menurunkan kualitas layanan multimedia. Penelitian ini ini membahas pengukuran dan analisa pengaruh routing protokol dan mekanisme keamanan pada kualitas layanan multimedia dengan menggunakan simulai aplikasi atau layanan VoIP sebagai ujicoba. Berdasarkan hasil simulasi didapatkan hasil pengaruh dari penerapan mekanisme keamanan pada layanan VoIP *delay* untuk komunikasi VoIP dengan media transmisi yang secure dan *delay* pada proses pensinyalan meningkat 4,22%.**

***Kata Kunci*— Quality of Service, Routing Protokol, TLS, SRTP, layangan multimedia secure.**

I. PENDAHULUAN

Layanan multimedia pada jaringan TCP/IP seperti teknologi *Voice Over IP* (VoIP) penggunaannya di internet terus meningkat. VoIP diadopsi oleh konsumen, perusahaan, dan operator telekomunikasi karena potensinya untuk fleksibilitas yang lebih tinggi, rangkaian fitur yang lebih kaya, dan dari segi biaya yang relative lebih murah dibandingkan dengan GSM dan *Public Switched Telephone Network* (PSTN). VoIP adalah teknologi yang digunakan untuk mentransmisikan suara lewat paket data pada jaringan IP (*internet protocol*). Ide ini menjadi salah satu tren terpenting dalam telekomunikasi. Seperti karakteris tik suatu teknologi VoIP menawarkan baik peluang atau kemudahan dan risiko keamanan, sehingga implementasi dari teknologi yang mengadopsi *IP telephony* perlu mempertimbangkan secara serius implikasi keamanannya.

Ada banyak cara untuk mengamankan VoIP dan aplikasi multimedia pada jaringan IP, seperti penggunaan protokol MIKEY, S / MIME, SRTP, TLS, dan IPsec [1]. Sedangkan akibat dari penggunaan protokol keamanan pada layanan atau aplikasi multimedia seperti VoIP pada jaringan, seperti yang dibahas sebelumnya akan berprngaruh terhadap kinerja VoIP dengan meningkatkan *latency*, *jitter* dan / atau packet *loss* [2]. Mekanisme keamanan menerapkan fungsi kriptografi ke paket akibatnya meningkatn *delay* untuk proses enkripsi dan dekripsi paket, algoritma yang lebih kuat akan menghasilkan *delay* yang lebih besar. Mekanisme keamanan juga meningkatkan penundaan panggilan karena mekanisme identifikasi dan otentikasi, meningkatkan *delay* dan *jitter* selama panggilan saat paket VoIP melewati jaringan yang menggunakan protocol keamanan.Mekansime keamanan seperti IPsec yang diimplementasikan di *router* untuk menyediakan tunnel atau terowongan yang aman untuk lalu lintas antar pengguna akhir, demikian juga dengan protokol keamanan lainnya seperti ZRTP, SRTP dan TLS juga menyebabkan *delay* dalam pengiriman paket..

Selain penggunaan mekanisme keamanan protokol routing pada jaringan juga dapat menyebabkan penurunan kualitas layanan. Beberapa menelitian mengemukakan hasil seperti: Metode *routing distance vector* jenis *Enhanced Interior Gateway Routing Protocol* (EIGRP) lebih cepat dibandingkan dengan *link state* jenis *Open Shortest Path First* (OSPF) [4], dan [8] mengemukakan bahwa metode routing distance vector jenis EIGRP lebih cepat dibandingkan dengan link state jenis OSPF.

Pada aplikasi multimedia *Quality of Service* (QoS) yang diberikan kepada pengguna sangat penting, karena jika percakapan dalam bentuk suara ataupun video tidak dapat dimengerti maka tidak ada gunanya menyediakan layanan ini. Faktor utama yang mempengaruhi QoS adalah *Latency*, *Jitter* dan Packet *loss* beberapa penelitian untuk menilai kualitas layanan suara telah diajukan. [6] memberikan tinjauan untuk pendekatan model penilaian dengan metodologi subyektif melibatkan eksperimen dengan subyek manusia seperti Mean Option Score (MOS)]. [7] Motode lain yang banyak digunakan yaitu penggunaan simulasi untuk memperkirakan kualitas yang dirasakan pengguna melalui pengukuran objektif, tanpa melibatkan subyek manusia. Metode simulasi untuk pengukuran dan validasi cukup populer untuk estimasi kinerja awal.

Penelitian ini ini membahas pengukuran dan analisa pengaruh routing protokol dan mekanisme keamanan pada kualitas layanan multimedia dengan menggunakan simulasi aplikasi atau layanan VoIP sebagai ujicoba.

II. KAJIAN PUSTAKA

A. Keamanan Voip

Kerahasiaan dalam komunikasi VoIP dicapai dengan menggunakan mekanisme keamanan. Ada dua fungsi pada VoIP yang harus dilindungi saat proses komunikasi melalui jaringan IP yaitu: proses pensinyalan (*signaling*) dan media transfer(komunikasi data) [5].

B. Proses Signaling

Session Initiation Protocol -SIP- adalah protokol pensinyalan IETF yang digunakan untuk membuat, memodifikasi, dan mengakhiri sesi panggilan melalui jaringan IP. Proteksi SIP biasanya dicapai dengan penggunaan dua protokol: *Transport Layer Security*(TLS dan *Secure/ Multipurpose Internet Mail Extensions* (S/MIME). TLS direkomendasikan oleh IETF di RFC 4346 [11] untuk mencegah serangan penyadapan, manipulasi pesan, dan pengulangan pesan [10].

TLS menawarkan otentikasi antara klien dan server untuk mencapai kerahasiaan dan integritas selama pertukaran informasi. TLS disusun oleh dua lapisan. Protokol lapisan rekam TLS menjaga koneksi aman antar terminal. Negosiasi bersertifikat yang menggunakan algoritma kriptografi harus diselesaikan sebelum pengiriman data dimulai dan merupakan tanggung jawab lapisan atas, protokol TLS [3]

C. Algoritma media enkripsi transmisi data

Untuk mengamankan proses pengiriman data atau paket data pada jaringan IP, aplikasi multimedia dengan audio, video atau kombinasi, menggunakan algoritma enkripsi untuk transmisi yang aman dan membuat saluran aman antara pengguna *end to end* [12].

D. SRTP

Secure Real Time Protocol (SRTP) adalah protokol yang mewakili otentikasi real-time, kerahasiaan dan integritas untuk lalu lintas multimedia, dan dijelaskan oleh RFC 3711 [3]. SRTP memberikan perlindungan dengan kunci enkripsi untuk jaringan kabel dan nirkabel termasuk saluran terbatas bandwidth [9].

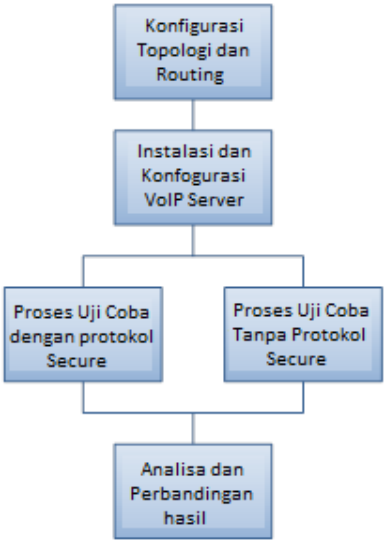
III. METODOLOGI

Penelitian ini meneliti kinerja VoIP yang dengan menggunakan protokol keamanan sebagai transport protokol, dengan menggunakan pendekatan simulasi.

A. Proses Simulasi

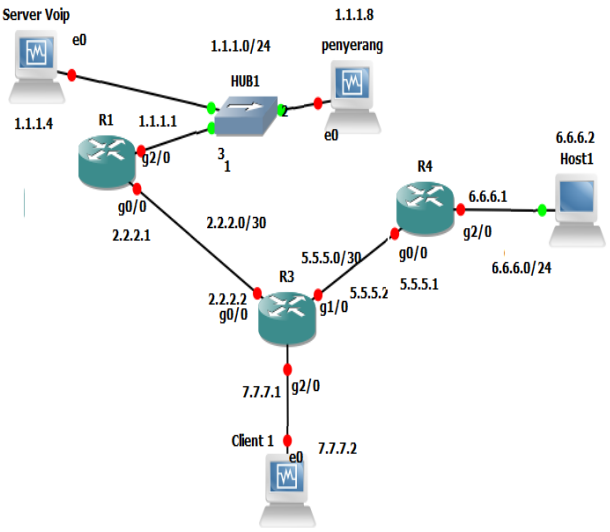
Perancangan sistem server VoIP menggunakan virtual box dengan sistem operasi Ubuntu 14:04, konfigurasi routing menggunakan simulator GNS3. Routing dinamis menggunakan tiga protokol routing seperti RIPv2, EIGRP, dan OSPF. Asterisk server VoIP menggunakan mekanisme keamanan TLS untuk *signaling* dan SRTP untuk sesi komunikasi data.

Proses simulasi untuk pengukuran kinerja VoIP seperti yang ditunjukkan pada gambar 1. Dua skenario dirancang, pada skenario pertama kualitas suara diperiksa dengan mengukur *delay* dan *jitter* dalam komunikasi VoIP yang aman, yang menggunakan mekanisme keamanan. Pengukuran skenario kedua tanpa menerapkan mekanisme keamanan. Kedua skenario menggunakan tiga *dynamic routing protocol* secara bergantian



Gambar 1. Metodologi yang digunakan

Gambar 2 menunjukkan topologi yang digunakan dalam simulasi dibangun menggunakan simulator GNS3. *Router* Cisco 7200 series untuk paket routing terhubung dengan Ethernet gigabyte.



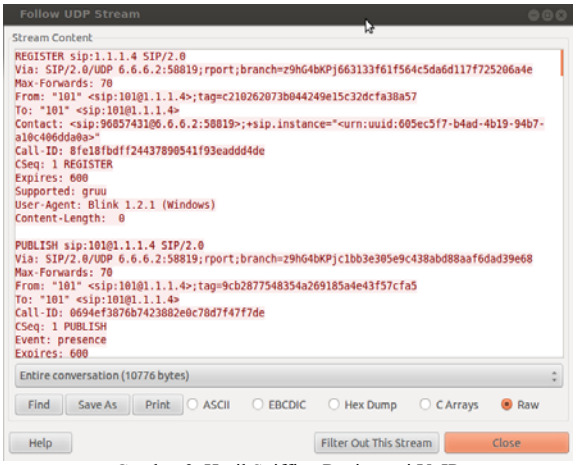
Gambar 2. Topologi Simulasi

IV. HASIL DAN PEMBAHASAN

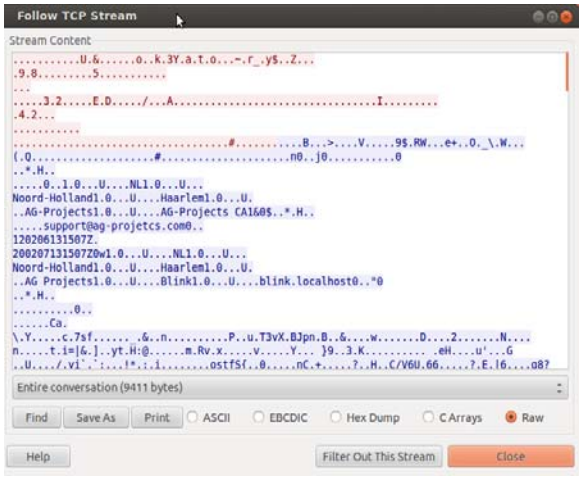
A. Proses Signaling VoIP

Untuk melihat implementasi keamanan dalam proses *signaling* dilakukan dengan cara mengendus(*sniffing*) paket

VoIP menggunakan wireshark. Gambar 3 dan 4 menampilkan hasil pada proses *sniffing* pada proses pensinyalan.



Gambar 3. Hasil Sniffing Registerasi VoIP



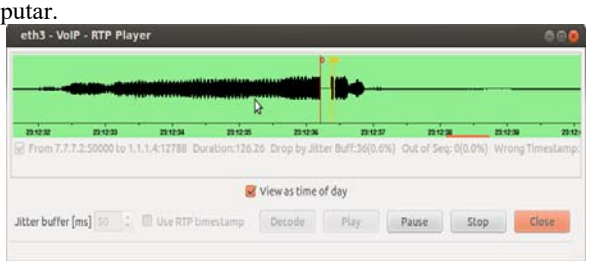
Gambar 4. Hasil sniffing registerasi VoIP ketika menggunakan secure protokol

Gambar 3 menunjukkan proses registrasi pada VoIP, Wireshark dapat membaca dan menampilkan informasi proses login dari IP 6.6.6.2 dengan user 101, hal ini terjadi karena paket tersebut tidak dienkripsi oleh protokol TLS.

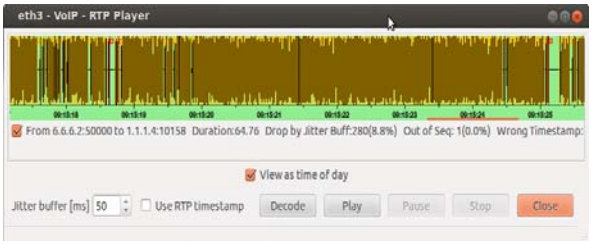
Gambar 4 menunjukkan hasil enkripsi untuk pendaftaran VoIP yang ditangkap oleh wireshark

B. *Data transfer pada VoIP*

Gambar 5 menampilkan paket RTP yang ditangkap oleh Wireshark, yang belum dienkripsi oleh protokol SRTP. Hasil sniffing bisa diputar ulang, percakapan dengan pengguna VoIP yang ditangkap oleh wireshark bisa terdengar dengan jelas. Gambar 6 menunjukkan paket RTP yang ditangkap oleh Wireshark, setelah dienkripsi oleh protokol keamanan SRTP. Pada gambar tersebut, grafik komunikasi terlihat berbeda dengan grafis pada komunikasi tanpa keamanan. Hasil sniffing dari paket terenkripsi menghasilkan suara yang tidak jelas dan banyak gangguan (*noise*) ketika diputar.



Gambar 5. Hasil capture paket RTP

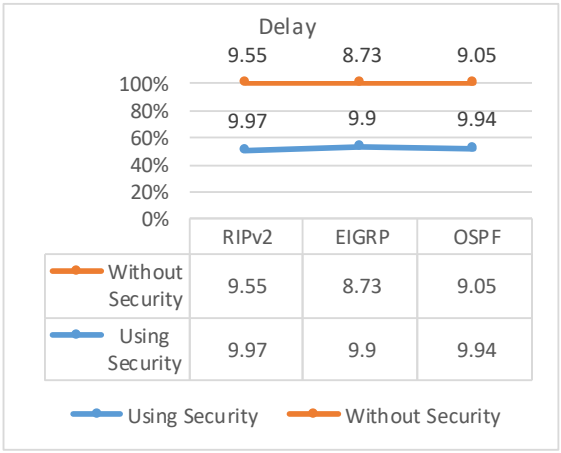


Gambar 6. Hasil capture paket SRTP

C. *Performa QoS*

Pengukuran kinerja QoS dilakukan dengan menggunakan beberapa skenario termasuk uji coba menggunakan mekanisme keamanan di VoIP, pengujian tanpa menggunakan mekanisme keamanan di VoIP dan menerapkan beberapa protokol routing dinamis pada jaringan.

Menguji mekanisme keamanan di VoIP dilakukan dengan menggunakan protokol TLS untuk proses pensinyalan *(call set-up*), menggunakan protokol SRTP untuk protokol transport, dan ASTERISK sebagai server VoIP. Protokol routing menggunakan tiga protokol dinamis yaitu RIPv2, EIGRP, dan OSPF. Hasil pengukuran kinerja ditunjukkan pada gambar 7 untuk perbandingan *delay*, angka 8 untuk hasil *jitter* dan perbandingan untuk packet *loss* pada gambar 9.



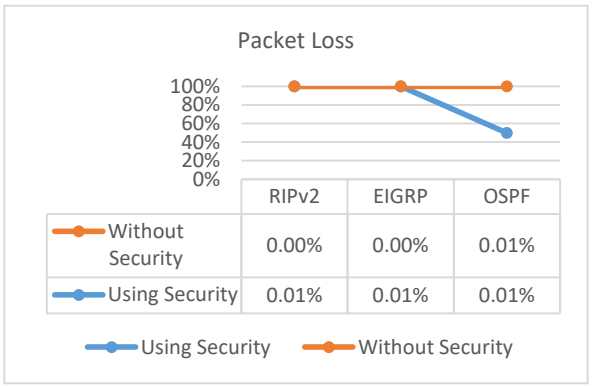
Gambar 7. Perbandingan *delay*

Dari gambar 7 rata-rata *delay* yang dihasilkan oleh komunikasi VoIP menggunakan mekanisme keamanan lebih tinggi daripada tanpa mekanisme keamanan. Sebagai

perbandingan penggunaan protokol routing dinamis Protokol routing EIGRP menghasilkan rata-rata *delay* terkecil.

Gambar 8. Perbandingan *Jitter*

Dari gambar 8 nilai *jitter* yang dihasilkan oleh komunikasi VoIP menggunakan mekanisme keamanan lebih tinggi dari *jitter* tanpa mekanisme keamanan. Hasil perbandingan untuk penggunaan protokol routing dinamis Protokol routing EIGRP menghasilkan *Jitter* terkecil.



Gambar 9. Perbandingan Packet *Loss*

Dari gambar 9 packet *loss* yang dihasilkan dengan menggunakan mekanisme keamanan lebih tinggi daripada tanpa mekanisme keamanan yang menghasilkan hampir tidak ada packet *loss* dengan kondisi jaringan uji coba tanpa background traffic.

TABLE-1.
VOIP QOS PERFORMANCE USING SECURITY MECHANISM.

Routing	*Delay*	*Jitter*	*Packet loss*
RIPv2	9,55 ms	0,91 ms	0.00 %
EIGRP	8,73 ms	0,39 ms	0,00 %
OSPF	9,05 ms	0,53 ms	0.01

D. *Pembahasan*

Seperti yang dibahas di bagian hasil, kinerja VoIP diambil untuk proses registrasi, pengaturan panggilan dan transmisi pada lalu lintas suara untuk memastikan ada efek buruk yang ditimbulkan akibat menggunakan mekanisme keamanan pada VoIP. Hasil yang didapat dari proses uji coba mekanisme keamanan menurunkan kualitas kinerja dengan meningkatkan *delay* dan packet *loss*.

Dari hasil simulasi didapatkan nilai *delay* pada VoIP dipengaruhi oleh penggunaan mekanisme keamanan, maka proses analisis diperlukan untuk menghitung *delay* yang dihasilkan oleh aplikasi multimedia. Perhitungan matematis diperlukan sebagai analisis awal keterlambatan yang dihasilkan oleh aplikasi multimedia. Proses selanjutnya yang direncanakan dalam penelitian ini adalah model matematis untuk model pengukuran *delay* multimedia.

V. KESIMPULAN

Berdasarkan hasil simulasi *delay* untuk komunikasi VoIP dengan media transmisi aman dan proses *signaling* meningkat 4,22%. Dari hasil simulasi didapatkan nilai *delay* pada VoIP dipengaruhi oleh penggunaan mekanisme keamanan dan protokol routing yang digunakan. Proses analisis lebih lanjut diperlukan untuk menghitung *delay* yang dihasilkan oleh aplikasi multimedia. Perhitungan matematis diperlukan sebagai analisis awal *delay* yang dihasilkan oleh aplikasi multimedia. Untuk pengembangan penelitian ini penggunaan model matematis untuk menghitung nilai *delay* akibat dari penggunaan mekanisme keamanan dan proses routing.

REFERENSI

[1] Bilien. J, Eliasson. E, Orrblad. J, and. Vatn. J O. 2005. Secure VoIP: Call Establishment andMedia Protection. In Proceedings of the 2nd Workshop on Securing Voice over IP, June.
[2] Barbieri. R, Bruschi.D, and Rosti. E. 2002. Voice over IPsec: Analysis and Solutions. In Proceedingsof the 18th Annual Computer Security Applications Conference (ACSAC), pages 261–270, December.
[3] Eren, Evren. Detken, Kai-Oliver. "Voice-over-IP Security Mechanisms– State_of:
[4] Fatkhurrokhman, M. 2013. Analisis Perbandingan Metode Routing Link State Vs Distance Vector
[5] Guillen, EP. Chacon, DA. 2009. VoIP Networks Performance Analysis with Encryption Systems. World Academy of Science, Engineering and Technology. 58
[6] Ismail, MN. 2009. Analyzing of MOS and Codec Selection for Voice over IP Technology. Anale. Seria Informatica. Vol. VII fasc. january.
[7] Jelassi, S. Rubino, G. Melvin, H. Youssef, H. Pujolle, G. 2012. Quality of experience of VoIP service: a survey of assessment approaches and open issues, IEEE Commun. Surveys Tutorials 14 (2) 491–513.
[8] Latubessy, A. Indrastanti R. Widiasari, Rissal Efendi. 2013. Analisis *delay* voice over internet protocol pada wide area network menggunakan single area open shortest path first routing protocol.
[9] Roberts. C. 2005 "Voice Over IP Security. Centre for Critical Infrastructure Protection". New Zealand.
[10] Rosenberg, J. Schulzrinne, H. Camarillo, G. Johnston, A. Peterson, J. Sparks, R. Handley, M. and Schooler. E. 2002. SIP: Session Initiation Protocol. IETF RFC 3261, June.
[11] Schulzrinne, H., Casner, S., Frederick R., Jacobson, V. 2003. "RTP: ATransport Protocol for Real-Time Applications". IETF RFC 3550. July.
[12] Thermos, P. A. Takanen. 2007. "Securing VoIP networks, Threats, Vulnerabilities, and Countermeasures". Addison Wesley. August.

[13] Wang, L. P. K. Verma, A Network Based Authentication Scheme for VoIP, School of Electrical and Computer Engineering University of Oklahoma, IEEE, Tulsa, OK, USA.