Steganografi pada VoIP dengan LACK

Salman M Ibadurrahman – NIM: 13506106

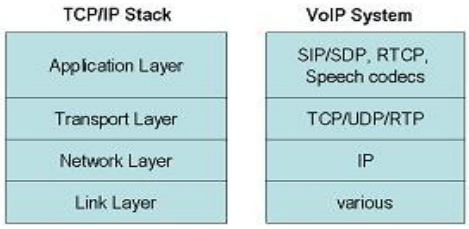
Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-Mail: if16106@students.if.itb.ac.id

Abstrak

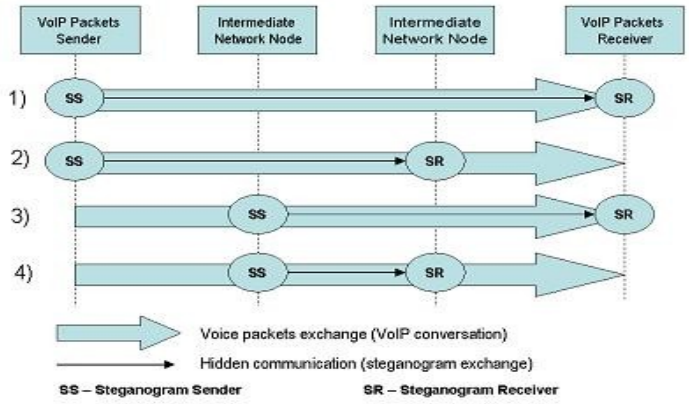
Makalah ini membahas tentang studi dan implementasi steganografi pada audio pada IP networking. Lebih spesifik, pada Voice Over Internet Protocol (VoIP) dengan metode (Lost Audio Packets Steganographic Method) LACK. LACK sebagai metode hybrid dalam melakukan steganografi terhadap data digital audio yaitu melakukan modifikasi terhadap data yang dikirmkan maupun melakukan delay terhadap sebagian paket data yang dikirim dari pengirim pesan VoIP ke pihak penerimanya. Bagaimana cara kerja dan kelebihan – kelebihan metode steganografi dengan LACK.

RTP (Real-time Transport Protocol) dan RTCP (Real-time Control Protocol) sebagai protocol yang digunakan dalam VoIP. Dalam VoIP banyak sekali hal – hal kritis yang menjadi bahan perhatian metode steganografi, diantaranya peluang terjadinya *congestion*, masalah keamanan, maupun masalah *realiability data.*

Kata kunci: LACK, VoIP, IP networking



Gambar 1 VoIP stack dan protokolnya



Gambar 2 skenario komunikasi tersembunyi pada VoIP

1. Pendahuluan

VoIP merupakan salah satu service yang populer di IP networking. Pertumbuhan pesat internet service yang semakin meningkat dari waktu ke waktunya, memicu kepadatan volume pada IP networking. Ini disebabkan oleh pengguna IP networking yang semakin banyak. Siapapun dapat menggunakan layanan ini. Salah satu isu yang muncul akibat banyaknya segmen pengguna layanan ini adalah masalah keamanan.

Keamanan menjadi isu yang sangat penting, karena inti dari layanan internet service adalah pengiriman data dari sebuah tempat ke tempat lain melalui IP networking. Dan IP networking merupakan jaringan yang sangat luas, mencakup seluruh dunia yang memungkinkan orang untuk mengaksesnya. Namun, Tidak semua orang berhak mengaksesnya. Yang berhak adalah orang yang mengirim data dan orang yang diharapkan menerima data tersebut. Orang yang mengakses data tersebut tetapi bukan merupakan orang yang berhak dinamakan pihak ketiga. Dan hal itu sangat tidak diharapkan.

VoIP merupakan salah satu aplikasi layanan IP networking. Tentu saja VoIP sangat diharapkan keamanannya, karena banyak sekali orang yang menggunakan layanan ini untuk berbicara lama dengan orang lain dan tentu saja pembicaraannya sangat tidak ingin diketahui oleh orang lain yang tidak berhak, karena mungkin saja pembicaraan tersebut berisi rahasia – rahasia, dan sebagainya.

Steganografi adalah proses penyembunyian data. Sedangkan steganografi pada VoIP adalah proses penyembunyian data suara yang diubah menjadi data digital yang dikirimkan ke penerima, lalu disembunyikan suapaya tidak ada pihak ketiga yang dapat mengakses data tersebut.

2. Alur Komunikasi VoIP

VoIP merupakan layanan real-time yang mengizinkan IP telepon dengan menggunakan protokol. Terdapat empat macam protokol utama yang menjadikan IP telepon menjadi mungkin, diantaranya:

1. *Signalling Protocol*, adalah protocol yang membuat, memodifikasi, dan memutuskan komunikasi antara pihak yang sedang berkomunikasi. Yang saat ini populer adalah Session Initiation Protocol (SIP).

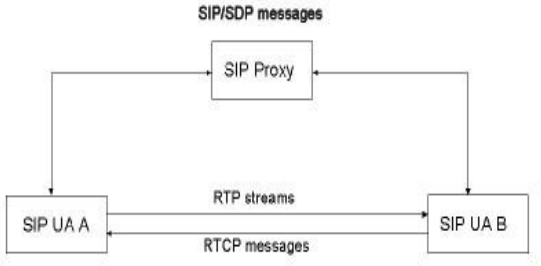
2. *Transport protocol* yang menyediakan *end-to-end connection*. Lebih dikenal dengan nama Real-time Transport Protocol (RTP). RTP menggunakan koneksi UDP atau terkadang menggukanan TCP untuk mengirimkan data digital suara.

3. *Speech codecs,* yaitu protocol yang bertugas melakukan kompresi/dekompresi data suara yang akan dikirimkan atau diterima melalui IP networking.

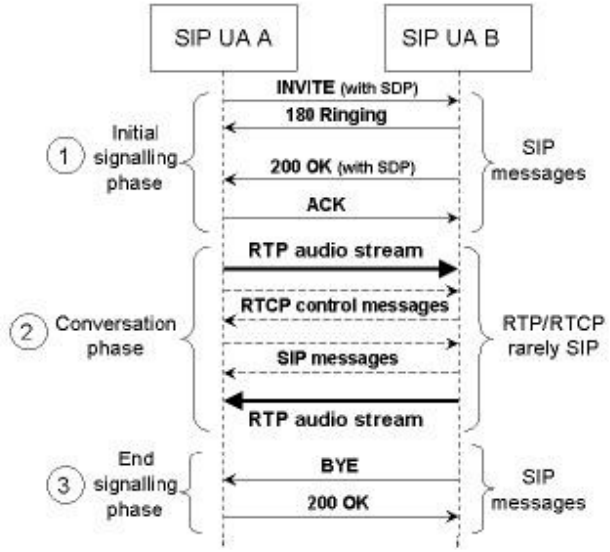
4. *Supplementary protocol*, yaitu protocol yang berisi fungsional – fungsional yang melengkapi fungsionalitas untuk bekerjanya layanan VoIP ini.

Secara umum, telepon IP terdiri dari dua fase, antara lain, *signalling phase* dan *conversation phase.* Pada kedua fase tersebut terjadi lalu lintas ataupun koneksi diantara pihak yang melakukan komunikasi dengan VoIP. Pada umumnya, fase *signaling phase* menggunakan SIP, sedangkan untuk transportasi audio dengan RTP. Pada saat terjadi proses *signaling*, terjadi pertukaran SIP *message* antara *end-point* pihak yang terlibaat dalam komunikasi VoIP. Setiap SIP *message* melalui SIP network server. Setelah fase *signaling* selesai, fase conversation dimulai. Yaitu, aliran audio (melalui RTP) dialirkan dari pihak pemanggil (*caller*) ke pihak yang dipanggil (*callee*).

Sebagai tambahan, RTCP merupakan control protocol bagi RTP dan di-desain untuk melakukan kualiti control atas servis dalam sebuah sesi komunikasi dengan VoIP.



Gambar 3 Gambaran umum protocol yang bekerja pada VoIP



Gambar 4 VoIP call setup dengan protokol SIP/RTP

3. Audio Watermarking

Audio watermarking adalah bentuk steganografi juga, yaitu menambahkan sesuatu pada data audio yang akan disamarkan aslinya. Inti dari hal ini adalah melakukan modifikasi terhadap konten data audio yang akan menjadi objek.

Kegunaan utama audio watermarking adalah menjaga hak intelektual atau menjaga keamanan dari data audio, atau dengan kata lain menjaga *Digital Right Management* (DRM).

4. Chanel tersembunyi pada VoIP

Ketika terjadi komunikasi melalui VoIP, pihak-pihak sebagai *end point* memiliki control atas masing-masing pihak tersebut. Yaitu, control yang melakukan modifikasi dan inspeksi terhadap paket yang diterima dan di-*generate* (yang telah diubah). Inilah yang menjadikan chanel ini menjadi disebut chanel tersembunyi.

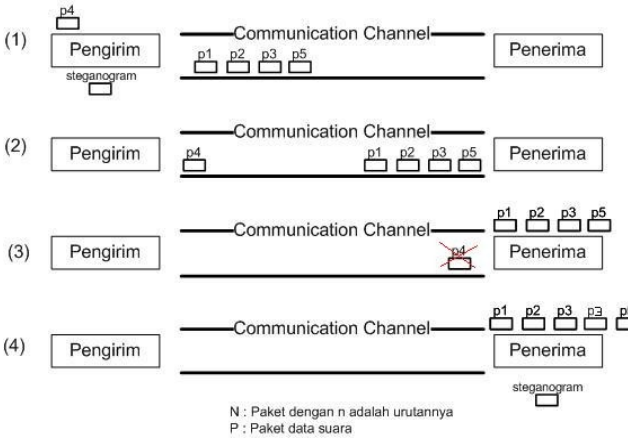
Terdapat tiga macam ukuran - ukuran yang menajdi karakteristik dari chanel tersembunyi ini, antara lain:

1. *Bandwith* yang menggambarkan banyaknya bits data yang dapat dikirimkan dalam satu satuan waktu..
2. *Total data yang disembunyikan pada chanel tersembunyi* adalah total bits data yang telah disembunyikan pada mekanisme steganografi VoIP.
3. *Distribusi data pada chanel tersembunyi*

5. Lost Audio Packets Steganographic Method

LACK adalah metode steganografi hybrid yang digunakan pada kelas multimedia pada skala besar, diantaranya RTP. Disebut hybrid karena dalam metode ini dilakukan modifikasi isi dari data maupun memanipulasi delay waktu (*offset*).

Ide utama dari metode LACK adalah sebagai berikut. Sebagian atau satu buah paket suara yang akan dikirimkan dipilih. Lalu di transmitter dengan sengaja diberikan delay (ditunda pengirimannya). Setelah paket lain dikirimkan, paket yang tadi dengan sengaja telah diberi delay oleh steganogram, baru dikirim menuju *receiver* dengan maksud, data – data yang berupa paket suara ketika di perjalanan/communication channel tidak lengkap dalam suatu waktu, agar apabila ada pihak ketiga yang mengambil paket – paket itu di tengah jalan, paket – paket data tersebut tidak berarti. Lalu paket yang tadi telah diberi delay dikirimkan ke receiver. Karena terdapat delay yang cukup lama, maka receiver tidak akan menganggap paket tersebut karena delaynya dianggap terlalu lama oleh receiver. Hal ini dilakukan dengan cara memilih parameter delay yang melebihi delay yang biasanya (delay paket lain). Berikut gambar yang menunjukan cara kerja LACK:



Gambar 5 Simulasi cara kerja LACK. Paket p4 diberi delay pada transmitter, lalu diabaikan oleh receiver.

Diperlukan beberapa pertimbangan dalam memilih delay sebagai parameter dalam steganografi dengan teknik LACK ini. Karena sangat diharapkan sekali, paket yang telah dipisahkan dan diberi delay tersebut benar – benar tidak akan dianggap oleh receiver untuk benar – benar menlaksanakan teknik ini. Detail analisis dan penjelasan pemilihan parameter, probabilitas prosedur dapat ditemukan di Mazurczyk and Lubacz, 2008.

6. Steganografi bergantung pada medium (LACK)

Steganografi pada VoIP menggunakan layer 1 atau layer 2 pada layer ISO OSI, yaitu layer *physical layer* atau *datalink layer*. Komunikasi via IP networking sangat bergantung pada medium, karena ini menyangkut *data rate, bandwith, error rate*, dan sebagainya. Terlebih pada metode steganografi LACK, berbeda medium, maka perhitungan parameter dan pemilihan prosedur pada metode ini akan berbeda. Kasus gagal bisa saja terjadi, sebagai contoh, paket yang telah diberi delay lebih, yang seharusnya dianggap hilang oleh receiver akhirnya bersatu kembali dengan paket lainnya yang memang harus diterima oleh receiver karena mediumnya memungkinkan paket yang tak diberi delay mengalami *congestion* sedangkan paket yang diberi delay tidak mengalaminya. Dan *timeout*-nya pun belum sampai, sehingga proses LACK ini gagal.

7. Analisa teknik steganografi LACK

Type of traffic	Percent [%]
SIP messages	0.016
RTP packets	99.899
RTCP reports	0.085

Tabel 1 Distribusi rata – rata data pada VoIP

Dari table 1 kita dapat melihat bahwa, metode steganografi yang menggunakan RTP paket menggunakan sekitar 99.9% lalu lintas VoIP.

Measure	Value	Standard Deviation
Average total amount of covert data	1364170 [bits]	4018.711
Average RBR	2487,80 [bits/s]	4.025
Average PRBR	50,04 [bits/packet]	2.258

Tabel 2 Hasil pengamatan dari sebuah panggilan pada VoIP

Keefektifan steganografi dengan LACK sangat bergantung pada banyak factor, antara lain, prosedur pada komunikasi seperti penggunaan *codecs*, besarnya ukuran frame data audio, besarnya buffer,

dan keadaan jaringan yang menyangkut delay, kemungkinan paket hilang, dan sebagainya.

Dari tabel 1 dapat dilihat bahwa, data yang mendominasi dalam komunikasi chanel tersembunyi pada VoIP adalah RTP. Karena RTP merupakan data-data yang terjadi ketika conversation fase, yaitu fase yang merupakan fase utama dalam komunikasi dengan VoIP. Dan sebagian data yang menjadi data tersembunyi harus dikirim lebih dari satu kali, karena metode LACK yang mengharuskan demikian.

8. Kesimpulan

Metode steganografi LACK merupakan metode yang cukup baru, mengingat teknologi VoIP atau voice pada IP networking merupakan teknologi baru. Metode ini cukup menawarkan fitur-fitur yang menjanjikan bagi keamanan transaksi data yang merupakan isu utama dalam IP networking. Dan implementasi LACK itu sendiri tidak begitu kompleks jika dibandingkan dengan metode– metode audio steganografi yang lainnya, seperti HICCUPS, SRTP, dan lain-lain. Yang menjadi masalah kritik Dalam aplikasi LACK adalah pemilihan prosedur (hal-hal yang berhubungan dengan kondisi networking) dan pemilihan parameter-parameter dalam pengiriman, diantaranya pemilihan parameter untuk menentukan delay.

Hal yang perlu dipertimbangkan dalam meng-implementasikan metode steganografi LACK ini diantaranya.harus diperhatikannya prosedur dan parameter-parameter yang akan digunakan dalam komunikasi VoIP, terutama pemilihan delay. Karena delay di sini cukup dilematis, karena apabila delay terlalu sebentar, ada kemungkinan mekanisme LACK tidak akan berjalan sempurna, namun apabila delay terlalu lama, maka delay pada pembicaraan antara dua pihak yang berkomunikasi akan cukup besar.

Akan tetapi, walalupun LACK sudah banyak digunakan, tetapi tidak menjamin bahwa LACK sudah sempurna dalam masalah keamanan. Apabila ukuran paket cukup besar, namun *Total data yang disembunyikan pada chanel tersembunyi* tidak besar, kemungkinan data diakses oleh pihak ketiga cukup terbuka.

Diperlukan pengembangan-pengembangan baru dalam metode ini. Karena metode dan ide ini cukup baik. Lalu mengingat perkembangan teknik *attacking* semakin hari semakin berkembang, maka diperlukan aktualisasi atau *upgrading* metode-metode yang sudah ada dan cukup baik saat ini.

Daftar Pustaka

[1] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[2] Tanenbaum, Andrew S. (2003). Computer Networks Fourth Edition. *Prentice Hall*

[3] http://www.theregister.co.uk/2008/06/03/voip_steganography/.*Tanggal akses: 27 maret 2009 pukul 09.00*

[4] *http://www.scmagazineuk.com/Steganography-harnesses-VoIP-networks/article/112101/.*

Tanggal akses: 27 maret 2009 pukul 09.00

[5] Mazurczyk, W., Szczypiorski, K., 2008b: Steganography of VoIP Streams. In: R. Meersman and Z. Tari (Eds.): TM 2008, Part II – Lecture Notes in Computer Science (LNCS) 5332, Springer-Verlag Berlin Heidelberg, Proc. of OnTheMove Federated Conferences and Workshops: The 3rd International Symposium on Information Security (IS'08), Monterrey, Mexico, November 9-14, 2008, pp. 1001-1018