**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNOLOGI INFORMASI**

**IINSTITUT TEKNOLOGI SEPULUH NOPEMBER**

**USULAN TUGAS AKHIR**

1. **IDENTITAS PENGUSUL**

**NAMA : Andarini Kartika Dewi**

**NRP : 5108 100 070**

**DOSEN WALI : Umi Laili Yuhana, S.Kom.,M.Sc.**

1. **JUDUL TUGAS AKHIR**

**2.1. Judul dalam Bahasa Indonesia :**

“*Analisis Pengiriman Frame Video Terenkripsi secara Unicast, Broadcast, dan Multicast”*

**2.2. Judul dalam Bahasa Inggris :**

“*Analysis on Encrypted Video Frame Delivery using Unicast, Broadcast, and Multicast*”

1. **LATAR BELAKANG**

Teknologi informasi saat ini mengalami perkembangan yang sangat pesat dari hari ke hari. Salah satu contoh keunggulan teknologi informasi adalah *video streaming*. *Video streaming* sebenarnya sebuah teknologi yang mempermudah kita dalam mendapatkan informasi dalam bentuk tampilan video. Pemanfaatan *video streaming* dapat berupa *video conference*. *Video conference* adalah telekomunikasi dengan menggunakan audio dan video sehingga terjadi pertemuan di tempat yang berbeda-beda. Ini bisa berupa antara dua lokasi yang berbeda (*point-to-point*) atau mengikutsertakan beberapa lokasi sekaligus di dalam satu ruangan konferensi (*multi-point*).

Teknologi *video conference* ini sangat efisien bagi perusahaan, terutama yang memiliki cabang-cabang perusahaan yang letaknya cukup jauh. Hal ini dikarenakan teknologi ini mengurangi biaya perusahaan yaitu biaya perjalanan untuk keperluan rapat atau pertemuan, biaya penginapan, konsumsi dll. Selain itu teknologi *video conference* ini dapat memungkinkan orang yang tidak dapat berpergian dapat saling berkomunikasi secara tatap muka.

Ada beberapa teknik yang biasa digunakan dalam pengiriman paket data video conference. Yang pertama adalah *unicast*, yaitu istilah untuk mendefinisikan suatu proses komunikasi dimana data informasi dikirimkan dari satu titik ke titik lain. Dalam *unicast* hanya ada satu pengirim dan satu penerima, atau paket data yang dikirimkan dari satu sumber ke satu tujuan. Yang kedua adalah *broadcast*, yaitu mengirimkan paket data, dalam hal ini video, kepada seluruh *host* yang ada. Teknik ini sering dipakai namun salah satu kekurangannya adalah *router* akan kebanjiran paket data. Untuk menghindari hal ini, dipakailah teknik *multicast*. *Multicast* yaitu mengirimkan paket data ke *host-host* yang tergabung dalam *group multicast*. Secara teori multicast dapat mengurangi beban lalu lintas pada jaringan.

Karena pentingnya fungsi *video conference* ini, maka kita membutuhkan saluran yang aman agar bisa melakukan *video conference* tanpa mendapat gangguan dari pihak-pihak yang tidak kita inginkan. Dengan melakukan enkripsi terhadap video yang ditransmisikan, *video conference* yang kita lakukan menjadi cukup aman. Di samping itu, karena aplikasi ini merupakan aplikasi yang bersifat *real-time*, untuk mengurangi waktu maka yang dienkripsi adalah *frame* videonya, bukan keseluruhan video. Dalam aplikasi video conference ini akan diimplementasikan algoritma enkripsi RC-5 (*Rivest Cipher-5*).

1. **TUJUAN**

Tujuan pembuatan tugas akhir ini adalah membandingkan performa pengiriman paket data secara *unicast*, *broadcast* dan *multicast* pada sebuah aplikasi *video conference* yang dilengkapi dengan enkripsi pada *frame* videonya. Keamanan pada aplikasi ini diwujudkan dengan menerapkan algoritma enkripsi RC-5 (*Rivest Cipher-5*) pada video yang ditrasmisikan. Sedangkan performa *unicast*, *broadcast* dan *multicast* yang dimaksud di sini adalah dalam hal *fps* (*frame-per-second*) dan *delay* yang terjadi.

1. **PERMASALAHAN**

Adapun yang menjadi permasalahan utama dalam tugas akhir ini :

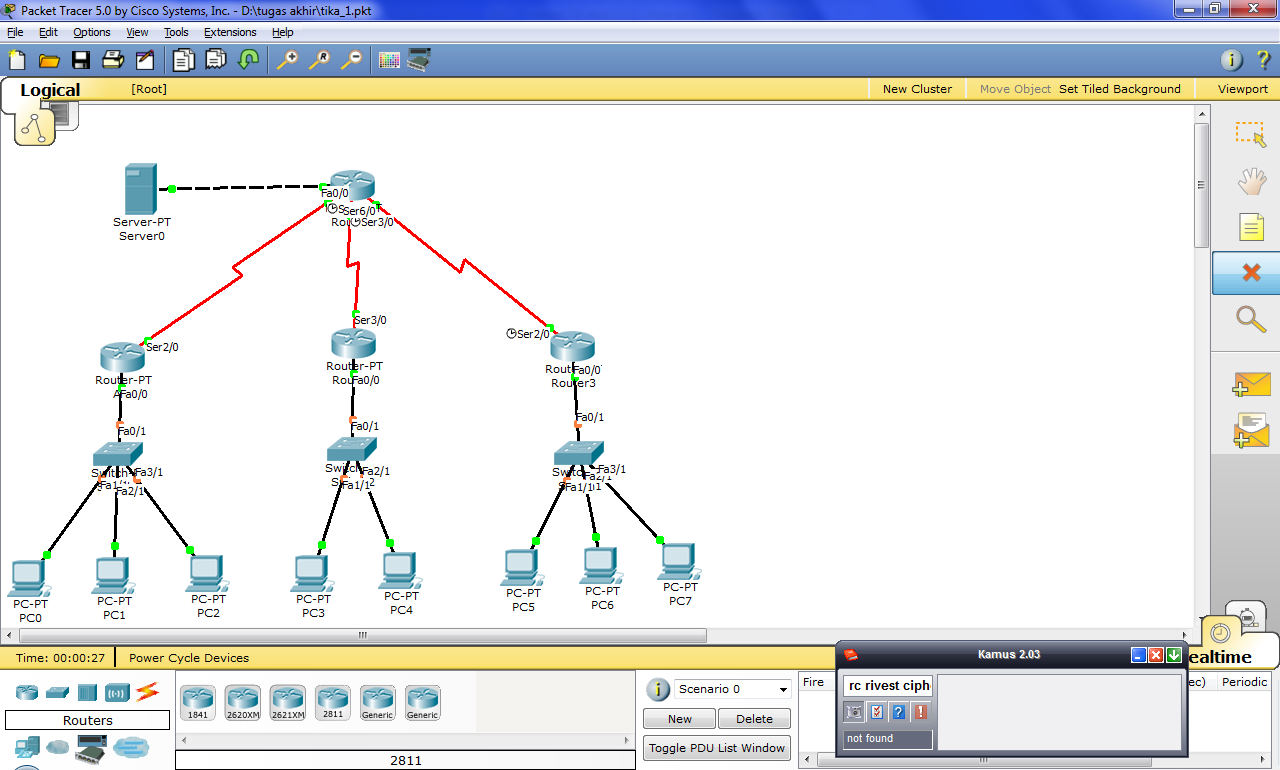
1. Bagaimana cara menerapkan algoritma enkripsi RC-5 (*Rivest Cipher-5*) yang akan digunakan pada setiap *frame* video?
2. Bagaimana cara memodifikasi agar data bisa terkirim ke penerima secara *unicast*, *broadcast* dan *multicast*?
3. **BATASAN MASALAH**

Dari permasalahan yang telah diuraikan di atas, terdapat beberapa batasan masalah terhadap tugas akhir ini, yaitu :

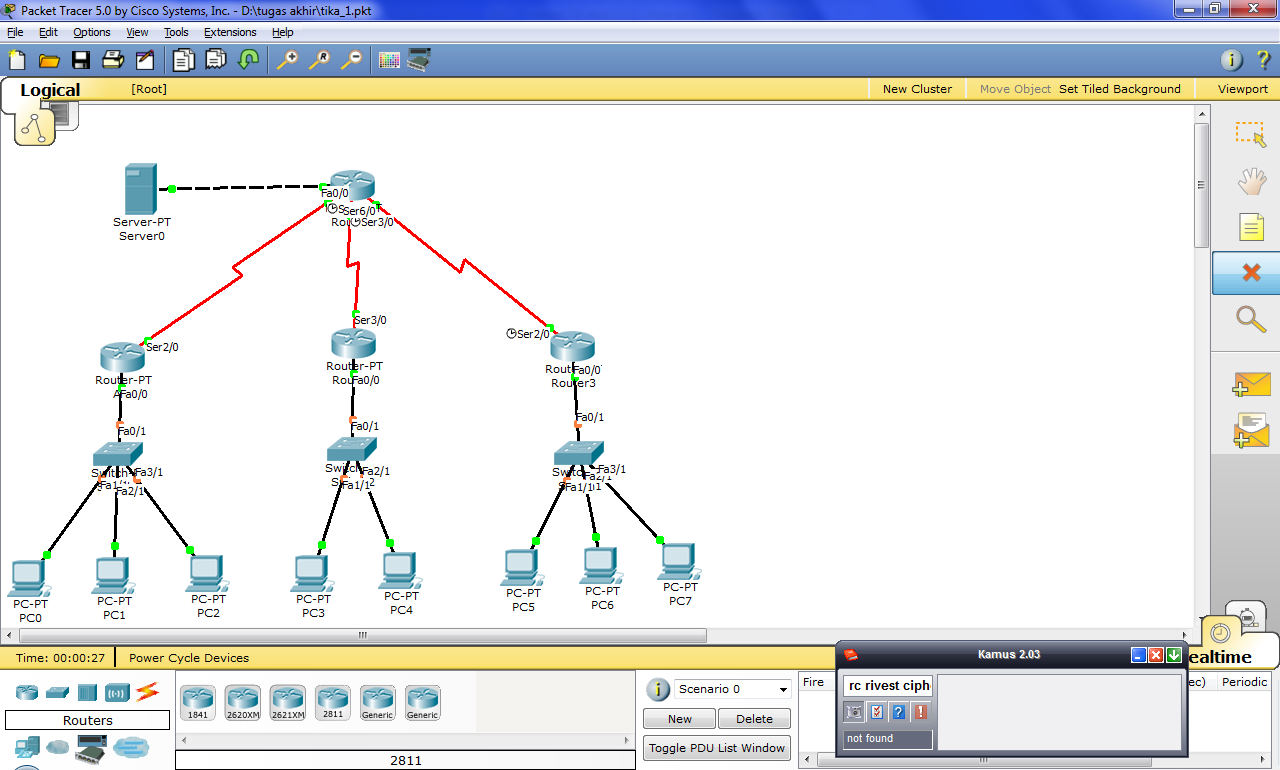
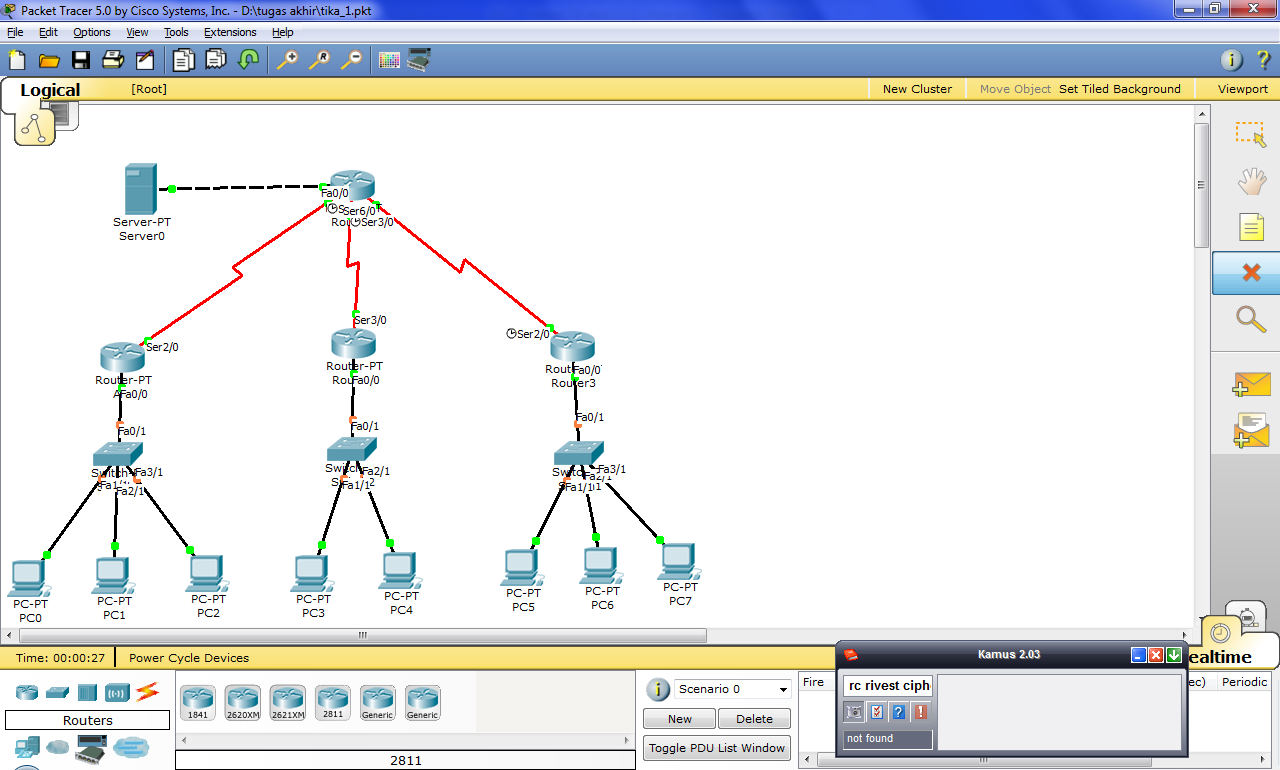
1. Format video yang digunakan dalam aplikasi ini adalah MPEG-1 dan MPEG-2.
2. Algoritma enkripsi yang digunakan untuk mengenkripsi dan mendekripsi frame video adalah RC-5 (*Rivest Cipher-5*).
3. Aplikasi ini merupakan aplikasi *video streaming* yang dapat menangkap gambar dan mengirim data *video stream*. Namun tidak melakukan operasi lanjutan misalnya *zoom*, *pan*, dan *tilt*, karena lebih menfokuskan dari sisi enkripsi pada video.
4. **RINGKASAN ISI TUGAS AKHIR**

Pada tugas akhir ini akan dibuat sebuah aplikasi *video conference.* Aplikasi ini bisa digunakan untuk menangkap gambar dari sebuah kamera digital secara *real-time* serta bisa mengirimkan video yang tidak bersifat *real-time*. Aplikasi ini berfungsi sebagai media komunikasi antara orang-orang yang berada pada lokasi yang berbeda, yang letaknya cukup berjauhan. Dengan adanya aplikasi ini, orang-orang yang mengadakan pertemuan tidak perlu berkumpul di suatu tempat yang sama pada waktu yang sama.

Aplikasi ini dapat mentransmisikan video secara *unicast*, *broadcast* dan *multicast*. *Unicast* berarti melakukan *video conference* antara dua komputer secara *point-to-point*. *Broadcast* berarti melakukan *video conference* dengan seluruh *host* yang ada di jaringan tersebut. Sedangkan *multicast* maksudnya yaitu mengirimkan video pada komputer-komputer yang terhubung dengan jaringan, yang memiliki IP *multicast* yang sama. Sehingga kita bisa memilih *client* mana saja yang bisa melakukan *video conference* dengan kita.



*(a)*



*(b) (c)*

*Gambar 1. Pengiriman paket data secara (a) Unicact, (b) Broadcast, dan (c) Multicast*

Namun salah satu gangguan yang berbahaya adalah jika terdapat orang-orang tidak diinginkan yang melakukan *eavesdropping* atau bahkan merusak isi video yang ditransmisikan melalui jaringan. Hal ini tentu sangat merugikan bagi pihak resmi yang melakukan *video conference*. Untuk mencegah hal ini, digunakanlah suatu algoritma enkripsi pada video, yaitu RC-5 (*Rivest Cipher-5*). *Transmitter* akan melakukan enkripsi RC-5 pada *frame* video, sebaliknya *receiver* akan mendekripsi *frame* video agar muncul tampilan video yang sebenarnya. Enkripsi dan dekripsi dilakukan pada *frame* video saja, agar delay yang terjadi tidak terlalu besar.

1. **METODOLOGI**

Metodologi yang akan dilakukan dalam Tugas Akhir ini memiliki beberapa tahapan, di antaranya sebagai berikut:

1. **Studi Literatur**

Tahap ini merupakan tahap pengumpulan informasi yang diperlukan untuk pengerjaan tugas akhir sekaligus mempelajarinya. Mulai dari pengumpulan literatur, diskusi, serta pemahaman topik tugas akhir di antaranya tentang :

1. *Video Streaming* melalui IP menggunakan Java Media Framework
2. Algoritma enkripsi RC-5 (*Rivest Cipher-5*)
3. *Unicast, multicast* dan *broadcast*
4. Penangkapan gambar melalui kamera digital
5. **Perancangan Sistem**

Pada tahap ini dilakukan analisa awal dan pendefinisian kebutuhan sistem untuk mengetahui masalah yang sedang dihadapi. Dari proses tersebut selanjutnya dirumuskan rancangan sistem yang dapat memberi permecahan masalah tersebut.

1. **Implementasi**

Pada tahap implementasi ini akan dilakukan proses pembuatan aplikasi *video conference* beserta penerapan algoritma enkripsi dan dekripsi pada *frame* video. Selain itu dilakukan pengaturan pada jaringan agar aplikasi ini bisa melaksanakan *video conference* secara *unicast*, *broadcast* dan *multicast*.

1. **Pengujian dan Evaluasi**

Pengujian aplikasi ini dapat dilakukan antara lain sebagai berikut:

1. aplikasi dapat menangkap gambar dari kamera kemudian diolah menjadi video lalu mengirimkannya secara *real-time*, serta dapat mengirimkan video yang tidak bersifat *real-time*
2. aplikasi yang bertugas mengirimkan video (*transmitter*) bisa melakukan enkripsi pada *frame* video sebelum ditransmisikan melalui jaringan
3. aplikasi yang bertugas menerima video *(receiver*) bisa melakukan dekripsi pada *frame* video setelah menerima video melalui jaringan
4. aplikasi bisa mengirimkan video terenkripsi pada beberapa komputer secara *unicast*, *broadcast* dan *multicast*
5. **Penyusunan Buku Tugas Akhir**

Tahap terakhir merupakan penyusunan laporan yang memuat dokumentasi mengenai pembuatan serta hasil dari ujicoba dari perangkat lunak yang telah dibuat. Secara garis besar, Buku Tugas Akhir yang nantinya akan dibuat terdiri dari beberapa bagian antara lain

1. Pendahuluan
   1. Latar Belakang
   2. Permasalahan
   3. Batasan Tugas Akhir
   4. Tujuan
   5. Metodologi
2. Tinjauan Pustaka
3. Desain dan Implementasi
4. Uji Coba dan Evaluasi
5. Kesimpulan dan Saran
6. Daftar Pustaka
7. **JADWAL KEGIATAN**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Kegiatan** | **Bulan** | | | | | | | | | | | | | | | | | |
| **1** | | | | **2** | | | | **3** | | | | | **4** | | | | |
| 1. | Studi Literatur |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
| 2. | Perancangan Sistem |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
| 3. | Implementasi & Pembuatan Sistem |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
| 4. | Uji Coba dan Evaluasi |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
| 5. | Penyusunan Buku Tugas Akhir |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |

Keterangan : Bulan 1 dimulai pada Oktober 2011

1. **DAFTAR PUSTAKA**

[1] Ze-Nian Li, Mark S. Drew. Fundamentals of Multimedia. Washington: Pearson Education Inc.; 2004

[2] William Stallings. Cryptography and Network Security. Upper Saddle River: Prentice Hall; 2006

[3] Gabriele Oligeri, Stefano Chessa, Gaetano Giunta. Loss Tolerant Video Streaming Authentication in Heterogeneous Wireless Networks. Universita di Pisa; 2010

[4] C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan, C.V. Jawahar. Fast and Secure Real-Time Video Encryption. IEEE Computer Society; 2008

[5] IP Routing Fundamentals. Cisco Press Publications; 1999

**LEMBAR PENGESAHAN**

Surabaya, Oktober 2011

Mengetahui/Menyetujui,

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | Dosen Pembimbing I | Dosen Pembimbing II | |  |  | | **Ary Mazharuddin S, S.Kom., M.Comp.Sc.**  NIP. 19810620 200501 1 003 | **Baskoro Adi Pratomo,S.Kom.,M.Kom**  NIP. 510000003 | | |
|  |