Μακαλαη Σεμιναρ Τυγασ Ακηιρ

VISUALISASI PROSES OTENTIFIKASI PADA SISTEM KOMUNIKASI GSM (*GLOBAL SYSTEM FOR MOBILE COMMUNICATION*)

Ολεη: Μ Ριζα Μιηαρφα Τανφυνγ (Λ2Φ097654)
ριζα_τανφυνγ≡ψαηοο.χομ
Θυρυσαν Τεκνικ Ελεκτρο Φακυλτασ Τεκνικ Υνιϖερσιτασ Διπονεγορο

ABSTRAK

Sistem komunikasi bergerak seluler GSM media transmisinya tidak menggunakan kawat melainkan melalui gelombang radio, oleh karena itu faktor keamanan merupakan masalah yang sangat penting dan perlu diperhatikan dengan seksama. Adapun fungsi keamanan yang diterapkan dalam sistem komunikasi seluler GSM adalah proteksi identitas pelanggan, penyamaran data (ciphering) dan otentifikasi pelanggan.

Pada tugas akhir ini akan dipelajari dan dibahas salah satu aspek keamanan dari sistem GSM yaitu otentifikasi pelanggan, otentifikasi pelanggan dapat terjadi pada saat adanya permintaan registerasi lokasi maupun pembaharuan lokasi saat mobile station memasuki lokasi area baru dengan VLR yang berbeda. Untuk membantu memahami proses otentifikasi pelanggan, tugas akhir ini dilengkapi dengan program bantu visualisasi.

I. PENDAHULUAN

1.1 Latar Belakang

Telekomunikasi bergerak seluler merupakan salah satu sistem telekomunikasi yang sangat populer sejak dua dekade terakhir dan berkembang dengan sangat pesat, dimulai dengan diperkenalkannya sistem komunikasi seluler generasi pertama, yaitu AMPS yang merupakan sistem komunikasi selular analog sampai diperkenalkannya sistem seluler yang paling banyak digunakan di dunia yaitu sistem GSM yang merupakan sistem seluler digital. Sistem komunikasi bergerak ini berkembang dengan pesat seiring dengan tuntutan mobilitas, efektifitas dan efisiensi waktu yang tinggi.

Sistem komunikasi bergerak seluler digital memiliki keunggulan dibandingkan dengan sistem komunikasi bergerak analog, diantaranya dari aspek keamanan yang lebih sulit untuk dibajak. Sistem komunikasi bergerak seluler GSM media transmisinya tidak menggunakan kawat melainkan melalui gelombang radio, oleh karena itu faktor keamanan merupakan masalah yang sangat penting dan perlu diperhatikan dengan seksama. Adapun fungsi keamanan yang diterapkan dalam sistem komunikasi seluler GSM adalah proteksi identitas pelanggan, penyamaran data (*ciphering*) dan otentifikasi pelanggan. Penyamaran data dilakukan mengingat komunikasi yamg melalui transmisi gelombang radio yang terjadi sangat rentan terhadap penyadapan informasi. Proses otentifikasi merupakan suatu proses pemeriksaan keabsahan pelanggan, proses ini memberikan jaminan keamanan bagi pelanggan maupun bagi jaringan sebab dengan adanya otentifikasi hanya pelanggan yang terdaftar saja yang dapat menggunakan jaringan dan dapat melindungi akses jaringan dari pihak lain yang tidak sah.

1.2 Tujuan

Pada tugas akhir ini akan dipelajari salah satu bagian pengaturan keamanan sistem komunikasi seluler GSM 900/1800, yaitu proses otentifikasi.. Untuk memperjelas proses otentifikasi digunakan program bantu visualisasinya sehingga peminat studi ini memperoleh gambaran yang jelas.

1.3 Batasan Masalah

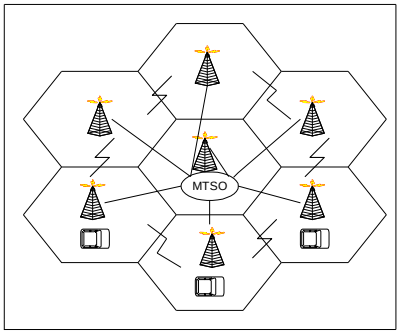
Karena begitu luasnya cakupan pada sistem komunikasi seluler GSM, maka penyusun membatasi masalah dengan hanya membahas proses otentifikasi pelanggan pada sistem komunikasi GSM dengan menggunakan algoritma otentifikasi DES. Pembuatan program bantu visualisasi tidak dibahas secara mendalam.

II. SISTEM KOMUNIKASI GSM

2.1 Konsep Seluler

Komunikasi bergerak dapat didefinisikan sebagai komunikasi antara dua terminal yang salah satu atau keduanya bergerak. Dalam sistem radio seluler, suatu wilayah geografi dibagi menjadi beberapa *cluster* atau *cell*. Besarnya sel ini bergantung pada kapasitas trafik yang diinginkan. Semakin banyak sel yang

dibutuhkan maka semakin besar pula kapasitas yang diharapkan yang berarti sel semakin rapat. Untuk melayani pemakai dalam komunikasi bergerak seluler, dibutuhkan sedikitnya satu stasiun induk (*Base Station*) berupa menara yang menghubungkan satu pemakai dengan pemakai lain dan yang menjadi pencatu (*feeder*) bagi terminal yang lainnya, seperti yang terlihat pada Gambar 2.1.



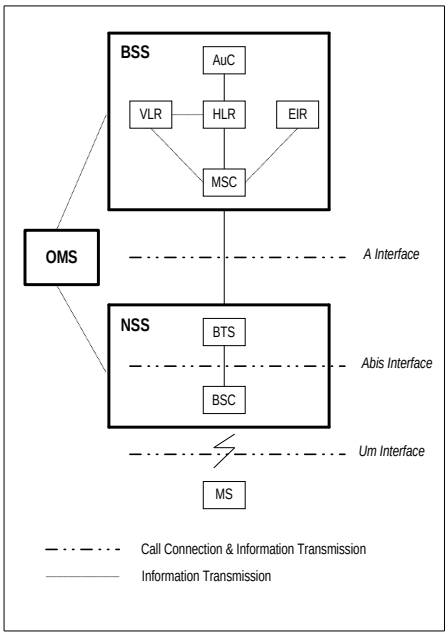
Gambar 2.1 Konsep Sistem Seluler

Stasiun Induk Radio (*Radio Base Station*) akan melayani satu daerah cakupan yang jarak atau luasnya bergantung pada tinggi menara, sifat antena yang digunakan dan batas daya yang diperkenankan diterima oleh pemakai bergerak. Secara konseptual sebuah sel digambarkan dalam bentuk heksagonal, namun bentuk seperti ini hanya fiktif sebab bentuk heksagonal itu digunakan untuk memudahkan perancangan saja dan untuk menggambarkan adanya daerah batas antar sel (*handover*), pada kenyataannya daerah cakupan dalam satu sel tidak heksagonal melainkan berbentuk tidak beraturan.

2.2 Arsitektur GSM

Jaringan GSM secara garis besar seperti yang tampak pada Gambar 2.3 dibagi menjadi tiga subsistem berikut.

- *Radio Subsystem / Base Station Subsystem* (BSS), merupakan interface antara jaringan dengan pengguna yang meliputi fungsi dan peralatan yang berkaitan dengan pengaturan hubungan pada jalur radio, termasuk *handover*. Untuk menunjang komunikasi, maka pengguna membutuhkan suatu *hardware* berupa *mobile station* (MS
- *Network Switching Subsystem* (NSS), subsistem jaringan merupakan interface jaringan GSM dengan jaringan lainnya seperti PSTN dan ISDN. Subsistem ini meliputi peralatan dan fungsi yang berhubungan dengan panggilan ujung ke ujung, manajemen mobilitas pelanggan
- *Operation and Maintenance Subsystem* (OMS), subsistem operasi merupakan interface dengan operator yang meliputi peralatan operasi dan pemeliharaan



Gambar 2.2 Arsitektur Jaringan GSM

2.3 Representasi Kanal

Representasi kanal pada sistem GSM menggabungkan akses sistem dalam ranah waktu dan frekuensi. Dalam ranah frekuensi atau disebut sistem FDMA (*Frekuensi Division Multiple Access*) sistem GSM mempunyai lebar bidang frekuensi yang digunakan sebesar 25 MHz berada pada frekuensi 890 – 915 MHz untuk arah *uplink* yaitu dari MS (*mobile station*) ke BS (*base station*), dan 935 – 960 MHz, untuk arah *downlink* yaitu dari BS ke MS.

2.3.1 Kanal Fisik

Secara Fisik 1 kanal frekuensi terdiri atas 8 *time slot*. 1 *time slot* dari TDMA frame mengacu pada 1 kanal frekuensi, sehingga pada sistem GSM terdapat 8 kanal tiap *carrier*, yaitu kanal 0-7. Lebar masing-masing kanal sebesar 200 KHz, sehingga untuk keseluruhan sistem GSM yang memiliki spektrum sebesar 25 MHz terdapat 1000 kanal untuk arah *uplink* dan *downlink*

2.3.2 Kanal *Logic*

Dalam sistem GSM terdapat beberapa tipe kanal *logic* yang terdiri atas:

- Kanal trafik (TCH) adalah dimana *speech* atau informasi dari *user* GSM yang telah diubah menjadi digital akan dipetakan ke dalam kanal fisik
- *Control Channel* (CCH) Kegunaan CCH sangat erat kaitannya dengan pensinyalan dan pengontrolan.

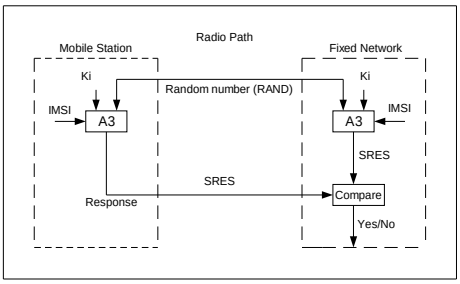
2.4 Penomoran pada Pelanggan

1. *Mobile Station ISDN Number* (MSISDN)
   MSISDN merupakan nomor yang diberikan oleh penyelenggara GSM kepada setiap pelanggan, diketahui oleh pelanggan dan tercatat di buku telepon, nomor inilah yang ditekan jika ada yang ingin menghubungi pelanggan GSM tersebut. Nomor ini disimpan secara permanen di dalam HLR
2. *International Mobile Subscriber Identity* (IMSI)
   IMSI merupakan nomor identitas pelanggan yang unik pada jaringan PLMN GSM. IMSI disimpan dalam HLR dan SIM *card* dari pelanggan yang bersangkutan
3. *Temporary Mobile Subcriber Identity* (TMSI)
   TMSI merupakan nomor identitas yang unik dari pelanggan yang tugasnya hampir sama dengan IMSI, namun bersifat sementara yang hanya dipergunakan di satu VLR saja. TMSI diberikan oleh VLR setelah *mobile station* pelanggan sukses melakukan proses otentifikasi. Nomor TMSI ini hanya berlaku untuk area yang dilayani oleh VLR tersebut.

III. OTENTIFIKASI PELANGGAN GSM

Sistem komunikasi GSM menyediakan beberapa fungsi keamanan, antara lain proteksi identitas pelanggan, enkripsi dan otentifikasi pelanggan.

Otentifikasi pelanggan dalam sistem GSM dilaksanakan dengan menggunakan suatu metoda yang bernama *challange response*. Metode ini dimulai dengan pengiriman suatu bilangan acak atau *random* ke *mobile station*. Kemudian bilangan ini diproses dengan algoritma otentifikasi A3 sehingga menghasilkan suatu bilangan *response* yang hasilnya akan dibandingkan dengan hasil perhitungan di jaringan, seperti yang tampak pada Gambar 3.1.

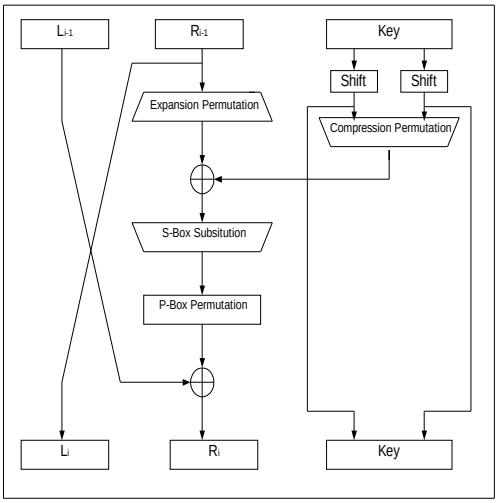


Gambar 3.1 Proses Otentifikasi Secara Umum

Pada otentitifikasi pelanggan penghitungan bilangan *SRes* dilaksanakan dengan menggunakan algoritma otentifikasi A3. Algoritma ini dalam penerapannya tidak memiliki standar dan berbeda untuk setiap penyelenggara layanan GSM serta algoritma ini dirahasiakan oleh masing-masing penyelenggara layanan GSM demi menjaga keamanan.

Karena algoritma A3 ini dirahasikan dan berbeda untuk tiap penyelenggara dan dirahasiakan, maka dalam Tugas Akhir ini dipergunakan suatu algoritma untuk menghasilkan bilangan SRes, yaitu algoritma DES.

Secara garis besar, algoritma DES terdiri dari 16 iterasi. Pertama sekali masukan data 64 bit ini masuk ke dalam IP (*initial permutation*), kemudian data masukam ini dibagi dua masing-masing 32 bit bagian kiri dan 32 bit bagian kanan. Terdapat 16 iterasi operasi yang sama, pada masing-masing iterasi diterapkan operasi dan kombinasi yang sama seperti yang tampak pada Gambar3.2.



Gambar 3.2 Satu *Round* DES

Algoritma berakhir setelah iterasi ke-16, data dari bagian kanan dan kiri digabungkan kembali kemudian diinverskan dengan IP (*initial permutation*).

Otentifikasi dalam sistem GSM dilaksanakan untuk melindungi jaringan PLMN GSM dari pihak –pihak lain yang tidak berhak menggunakannya. Elemen-elemen dari jaringan yang yang menjadi dasar dari pelaksanaan proses otentifikasi ini adalah VLR, HLR dan AuC. Otentifikasi pelanggan tersebut terjadi karena adanya beberapa permintaan prosedur dari mobile station seperti registrasi lokasi dan pembaharuan lokasi dengan perubahan VLR, otentifikasi pada prosedur tersebet kan dibahas secara mendetail pada subbab berikutnya.

IV. VISUALISASI DAN ANALISA OTENTIFIKASI PELANGGAN GSM

Program visualisasi otentifikasi pelanggan GSM ini terdiri dari suatu *form* menu utama, seperti yang terlihat pada Gambar 4.1.

Gambar 4.1 *Form* Menu Utama

Pada *form* menu utama tersebut terdapat tombol *OTENTIFIKASI PELANGGAN*, untuk memulai visualisasi tombol tersebut harus ditekan.

4.1 *Database* Pelanggan

Pengguna program ini harus dapat meregistrasikan diri pada jaringan program visualisasi melalui suatu akses *database*, untuk itu diperlukan suatu interface antara pengguna program dengan *database* agar pengguna dapat menambah, mengedit ataupun menghapus data-data pelanggan. Data pelanggan ini diperlukan pada saat pengguna akan memulai visualisasi proses otentifikasi pelanggan.

Program visualisasi ini telah menyediakan interface pengguna dengan *database* berupa sebuah form tersendiri, seperti yang terlihat pada Gambar 4.2, *form* ini secara langsung tersajikan apabila pengguna menekan tombol *OTENTIFIKASI PELANGGAN* pada *form* utama.

Gambar 4.2 *Database* Pelanggan

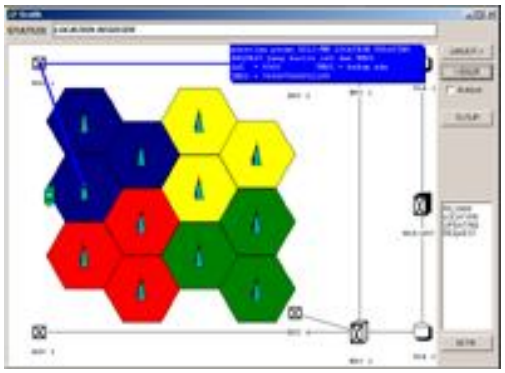
Data-data pelanggan yang harus dimasukkan ke dalam form *database* untuk menambah suatu daftar pelanggan adalah nama pelanggan, MISDN (*Mobile Station ISDN Number*) dan IMSI (*International Mobile Subscriber Identity*). Sedangkan kunci otentikasi pelanggan dibangkitkan oleh sistem untuk masing-masing pelanggan pada saat data pelanggan yang baru akan disimpan

4.2 Visualisasi Otentifikasi Pelanggan

otentifikasi pelanggan GSM oleh jaringan, yang dibahas dalam tugas akhir ini adalah yang terjadi pada dua hal yaitu : pada registrasi lokasi dan pembaharuan lokasi dari *mobile station* yang memasuki lokasi dengan VLR yang berbeda dengan VLR sebelumnya.

4.2.1 Otentifikasi pada Registrasi Lokasi

Registrasi lokasi terjadi pada saat mobile station diaktifkan pertama kali pada jaringan PLMN GSM, yaitu dengan memasukkan kartu SIM yang diperoleh dari penyelenggara ke dalam *mobile equipment* untuk melakukan penjelajahan untuk pertama kalinya. Adapun untuk memudahkan visualisasi dari proses registrasi lokasi ini diambil suatu jaringan sampel seperti yang terlihat pada Gambar 4.3. Kumpulan beberapa sel yang tergabung dalam suatu *location area* (LA) diberi warna yang sama, pada jaringan sampel tersebut terdapat empat buah *location area*. Masing-masing location area dikendalikan oleh sebuah BSC sehingga terdapat empat BSC. MSC satu memiliki *database* VLR 1 dan mengendalikan BSC 1 dan BSC 2, sedangkan MSC dua memiliki *database* VLR 2 dan mengendalikan BSC 3 dan BSC 4. *Location area* yang berada di atas, yaitu yang berwarna biru dan kuning ditangani oleh VLR 1 sedangkan *location area* yang berada di bawah ditangani oleh VLR 2.



Gambar 4.3 Otentifikasi pada Registerasi Lokasi

Pada visualisasi *location registration* ini posisi *mobile station* awalnya masih berada di

luar area layanan (di luar sel yang ada). Untuk memulai visualisasi *mobile station* harus diarahkan dan ditempatkan pada sel yang diinginkan. Selanjutnya program akan menunjukkan proses yang terjadi dan menampilkan pensinyalan berupa garis tebal berwarna biru atau merah, serta menampilkan keterangan dari proses yang sedang berlangsung. Setelah suatu tahap dijalankan, mode sinyal sampai ditujuan, pemakai harus menekan tombol *LANJUT* untuk melanjutkan proses dengan prosedur yang berikutnya, sedangakan tombol *BALIK* digunakan untuk kembali melihat proses sebelumnya. Sedangkan untuk melihat informasi yang terdapat pada masing-masing elemen jaringan yang berhubungan dapat dilakukan dengan menekan *mouse* pada posisi elemen jaringan tersebut.

Adapun proses *location registration* secara detail adalah sebagai berikut. Pada kondisi *location registration* ini kartu SIM belum memiliki TMSI (*Temporary Mobile Subscriber Identity*) dan kode LAI (*Location Area Identification*) yang disimpannya adalah 0. Oleh karena itu kemudian *mobile station* mengirimkan IMSI dan LAI-nya tersebut dalam bentuk tanpa penyamaran (*unciphered*) ke VLR melalui MSC dengan pesan pensinyalan *RIL3 -MM Location Updating Request*. Kode LAI yang dikirimkan dan telah diterima VLR bernilai 0 menunjukkan bahwa pelanggan tersebut tidak berasal dari area VLR yang lain. Kemudian VLR membuat data yang baru untuk pelanggan tersebut yang berupa LMSI (*Local Mobile Subscriber Identity)* yang dipergunakan untuk mempercepat akses data pelanggan. Dalam IMSI pelanggan yang diterima oleh VLR tadi terdapat alamat berupa kode HLR tempat pelanggan tersebut terdaftar.

Berdasarkan IMSI pelanggan tersebut VLR melakukan komunikasi dengan HLR dengan menggunakan interface D, komunikasi ini dilakukan dengan mengirimkan pesan pensinyalan *MAP/D Send Parameter* ke HLR yang bersangkutan yang berisi IMSI dan LMSI pelanggan untuk memperoleh parameter otentifikasi pelanggan di AuC. Pada AuC terdapat kunci otentifikasi Ki yang berpadanan dengan IMSI pelanggan, IMSI yang dikirimkan oleh VLR tersebut digunakan untuk mengakses Ki tersebut yang bersifat unik dan berbeda untuk setiap pelanggannya. Untuk permintaan otentifikasi yang pertama kali AuC belum memeliki satu set parameter atau *triplet* yang diminta oleh VLR, oleh karena itu AuC akan membangkitkan suatu bilangan random *Rand* untuk mendapatkan *triplet* (*Rand*, *SRes*, Kc) tersebut. Nilai *SRes* di AuC diperoleh melalui data masukan bilangan random *Rand* dan kunci otentifikasi Ki pelanggan dengan mempergunakan algoritma otentifikasi A3. Sedangkan nilai dari Kc diperoleh melalui perhitungan dengan algoritma A8 dengan masukan *Rand* dan Ki yang sama.

Satu set parameter *triplet* tersebut kemudian dikirimkan oleh HLR ke VLR dengan menggunakan interface D melalui pesan *MAP/D Send Parameter Result*, sehingga dalam database VLR telah tercatat nilai *Rand* dan *SRes mobile station* yang bersangkutan. Set parameter yang lainnya disimpan dalam *database* AuC untuk dipergunakan nanti apabila ada permintaan proses otentifikasi berikutnya. Kemudian VLR mengirimkan pesan *RIL3-MM Authentication Request* ke *mobile station* yang berisi bilangan random *Rand* yang meminta mobile station untuk menghitung bilangan *SRes'*. *Mobile station* menerima pesan tersebut, selanjutnya memerintahkan kartu SIM untuk menghitung *SRes'* menggunakan algoritma otentifikasi A3 yang terdapat pada SIM dengan pesan *SIM-ME Run GSM Algorithm.*

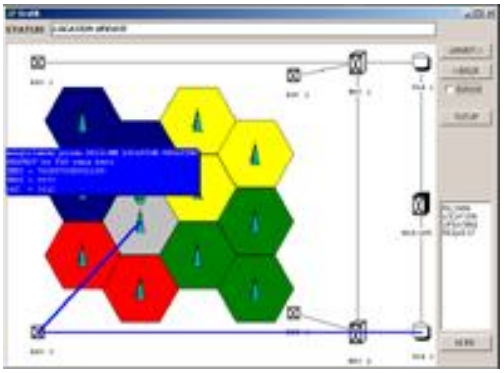
Setelah itu SRes' hasil perhitungan di dalam kartu SIM dikirimkan kembali ke VLR melalui pesan *RIL3 -MM Authentication Response.* Kemudian nilai *SRes'* yang dikirimkan oleh *mobile station* ini akan dibandingkan *SRes* hasil perhitungan di jaringan yang dikirimkan oleh AuC tadi, apabila kedua nilai *SRes* dan *SRes'* ini identik maka pelanggan dinyatakan sah dan proses *location registration* dilanjutkan dengan mengirimkan pesan *MAP/D Update Location* dari VLR ke HLR, pada tahap ini VLR mengirimkan data berupa IMSI dan nomor VLR yang menangani *mobile station* tersebut. Selanjutnya pesan *MAP/D Update Location Result* dikirimkan oleh HLR ke VLR yang bersangkutan, pesan ini merupakan pemberitahuan (*acknowledge*) ke VLR bahwa data yang dikirimkan tadi telah diterima oleh HLR, hubungan antara HLR dan VLR ini menggunakan interface D. Kemudian HLR mengirimkan pesan *MAP/D Insert Subscriber Data* ke VLR yang menangani *mobile station* tersebut, pesan ini berisi informasi IMSI dan MSISDN pelanggan yang bersangkutan. Selanjutnya VLR mengirimkan pemberitahuan (*acknowledge*) ke HLR yang menyatakan VLR telah menerima informasi yang dikirimkan melalui pesan *MAP/D Insert Subscriber Data*. Tahap selanjutnya adalah pengiriman pesan *RIL3 -MM Location Updating Accept* dari VLR ke *mobile station* yang bersangkutan, dalam pesan ini VLR mengirimkan data berupa nomor lokasi area LAI yang baru.

Kemudian VLR kembali mengirimkan pesan *RIL3-MM TMSI Reallocation Command* ke *mobile station* yang bersangkutan, pesan ini berisi nomor TMSI yang akan diberikannya kepada *mobile station.* Setelah pesan ini sampai, *mobile station* mengirimkan

pemberitahuan telah menerima TMSI dari VLR dengan mengirimkan pesan *RIL3-MM TMSI Reallocation Complete* ke VLR yang menanganinya, sehingga sekarang *mobile station* telah memiliki data-data IMSI, TMSI dan LAI yang dipergunakan untuk menjelajah pada area lokasi yang ditangani VLR yang bersangkutan

4.2.2 Otentifikasi pada Pembaharuan Lokasi dengan Perubahan VLR

Setelah *mobile station* sukses melaksanakan registrasi lokasi serta berhasil melakukan penjelajahan pada suatu *location area* yang ditangani oleh sebuah VLR dan akan memasuki *location area* baru yang ditangani oleh VLR lain yang berbeda maka jaringan akan melakukan prosedur pembaharuan lokasi dari *mobile station* yang bersangkutan. Program visualisasi pembaharuan lokasi ini menggunakan jaringan sampel dan *form* yang sama dengan visualisasi registrasi lokasi. Pada visualisasi pembaharuan lokasi ini, seperti yang terlihat pada Gambar 4.4, pengguna hanya memilih lokasi area yang baru yang berbeda VLR sehingga pengguna program visualisasi ini dapat melihat respon dari sistem pada saat memasuki lokasi area yang baru.



Gambar 4.4 Otentifikasi pada Pembaharuan Lokasi dengan Perubahan VLR

Adapun proses pembaharuan lokasi secara detail adalah sebagai berikut ini. Pada saat *mobile station* yang sedang aktif memasuki lokasi area baru yang memiliki VLR yang berbeda dengan VLR sebelumnya, MS tersebut menggunakan kanal logika SDCCH meminta pembaharuan lokasi melalui pesan *RIL3 -MM Location Updating Request* yang berisi kode TMSI dan LAI yang terdapat pada kartu SIM dan LAI yang baru diterimanya ke VLR dalam bentuk tanpa penyamaran (*unciphered*). VLR yang baru dalam hal ini VLR 2 menerima kode LAI tersebut dan mengevaluasinya, dari hasil evaluasi tersebut akan diketahui VLR sebelumnya yaitu VLR 1 tempat *mobile station* tersebut menjelajah yang terakhir. Setelah itu VLR 2 meminta VLR 1, dengan interface G, untuk mengirimkan parameter pelanggan yang bersangkutan melalui pesan *MAP/G Send Parameter* yang berisi kode TMSI yang diterima VLR 2 dari *mobile station*. VLR 2 juga membuat data yang baru yang dialamatkan dengan LMSI yang baru. Parameter yang diminta oleh VLR 2 dikirimkan oleh VLR 1 melalui pesan *MAP/G Send Parameter Result.*

Berdasarkan IMSI pelanggan yang diterima dari VLR 1, kemudian VLR 2 berhubungan dengan HLR/AuC dengan menggunakan interface D dan meminta parameter otentifikasi ke HLR/AuC dengan mengirimkan pesan *MAP/D Send Parameter* yang berisi IMSI pelanggan tersebut. Parameter yang diminta oleh VLR 2 dikirimkan oleh HLR/AuC melalui pesan *MAP/D Send Parameter Result* yang berisi set parameter triplet (*Rand*, *SRes*, Ki). Setelah menerima parameter tersebut dari AuC, VLR 2 melakukan proses otentifikasi terhadap pelanggan yang bersangkutan dengan mengirimkan pesan *RIL3 - MM Authentication Request* ke *mobile station*, selanjutnya proses otentifikasi sama seperti yang diuraikan pada kasus registrasi lokasi. Hasil perhitungan otentifikasi di *mobile station* berupa *SRes'* dikirimkan ke VLR melalui pesan *RIL3 - MM Authentication Response*, kemudian VLR akan membandingkan nilai *SRes* yang diterima dari HLR dengan nilai *SRes*' yang diterimanya dari *mobile station.*

Tahap selanjutnya dilaksanakan dengan mengirimkan pesan *MAP/D Update Location* dari VLR ke HLR, pada tahap ini VLR mengirimkan data berupa IMSI dan nomor VLR yang menangani *mobile station* tersebut. Selanjutnya pesan *MAP/D Update Location Result* dikirimkan oleh HLR ke VLR yang bersangkutan, pesan ini merupakan pemberitahuan (*acknowledge*) ke VLR bahwa data yang dikirimkan tadi telah diterima oleh HLR, hubungan antara HLR dan VLR ini menggunakan interface D. Kemudian HLR mengirimkan pesan *MAP/D Insert Subscriber Data* ke VLR yang menangani *mobile station* tersebut, pesan ini berisi informasi IMSI dan MSISDN pelanggan yang bersangkutan. Selanjutnya VLR mengirimkan pemberitahuan (*acknowledge*) ke HLR yang menyatakan VLR telah menerima informasi yang dikirimkan melalui pesan *MAP/D Insert Subscriber Data*. Tahap selanjutnya adalah pengiriman pesan *RIL3 -MM Location Updating Accept* dari VLR ke *mobile station* yang bersangkutan, dalam pesan ini VLR mengirimkan data berupa nomor lokasi area LAI yang baru.

Setelah pengiriman pesan *RIL3 -MM Location Updating Accept* dari VLR ke *mobile*

station, HLR akan berkomunikasi dengan VLR lama yang terakhir menangani *mobile station* tersebut dengan mengirimkan pesan *MAP/D Cancel Location*, pesan ini berisi perintah dari HLR kepada VLR yang lama untuk menghapus data-data *roaming* seperti LAI dan TMSI yang lama dari *mobile station* yang bersangkutan. Selanjutnya setelah melaksanakan perintah dari HLR tadi VLR yang lama mengirimkan pesan *MAP/D Cancel Location Result* yang memberitahukan bahwa data-data *roaming mobile station* yang bersangkutan telah dihapuskan dari *database*nya. Komunikasi kedua elemen ini dilakukan dengan menggunakan interface D

Kemudian VLR yang baru kembali mengirimkan pesan *RIL3-MM TMSI Reallocation Command* ke *mobile station* yang bersangkutan, pesan ini berisi nomor TMSI yang akan diberikannya kepada *mobile station*. Setelah pesan ini sampai, mobile station mengirimkan pemberitahuan telah menerima TMSI dari VLR dengan mengirimkan pesan *RIL3-MM TMSI Reallocation Complete* ke VLR yang menanganinya, sehingga sekarang *mobile station* telah memiliki data-data IMSI, TMSI dan LAI yang dipergunakan untuk menjelajah pada area lokasi yang ditangani VLR yang bersangkutan.

V. PENUTUP

5.1 Kesimpulan

Kesimpulan yang didapat dari Tugas Akhir dengan judul Visualisasi Proses Otentifikasi pada Sistem Komunikasi GSM (Global System for Mobile Communication) adalah sebagai berikut:

1. Sistem komunikasi GSM mensyaratkan adanya suatu proses pengesahan bagi pelanggan yang melakukan penjelajahan pada daerah layanannya demi menjamin keamanan pelanggan dan jaringan.
2. Otentifikasi pelanggan terjadi pada saat registerasi lokasi yaitu pada saat *mobile station* diaktifkan untuk pertama kalinya dan pada saat *mobile station* berpindah area lokasi dengan perubahan VLR
3. Otentifikasi pada GSM menggunakan metode *challange response*, yaitu jaringan memberikan suatu bilangan random ke mobile station kemudian mobile station memberikan responnya.
4. Program Visualisasi yang dibuat dapat berjalan dan menggambarkan proses otentifikasi pada sistem GSM.

5.2 Saran

Tugas akhir ini hanya membahas otentifikasi pelanggan pada registerasi lokasi dan pembaharuan lokasi saja, alangkah baiknya jika ada peminat studi ini yang mengembangkannya dengan membahas serta membuat program simulasi otentifikasi pada pembangunan hubungan dan aspek keamanan yang lain dalam sistem komunikasi GSM seperti proses penyamaran data.

DAFTAR PUSTAKA

[1] Bellamy. John, *Digital Telephony*, 2nd edition, John Wiley and Sons, New York,1991

[2] Dayeem. Rifaat A, *PCS and Digital CellularTechnology*, Prentice Hall PTR, New Jersey, 1997

[3] Garg. Vijay K & Wilkes. Joseph E, *Wireless and Personal Communication System*, Prentice Hall PTR, New Jersey, 1996

[4] Heine. Gunar, *GSM Network: Protocol, Terminology, and implementation*, Artech House Inc, Norwood, 1998

[5] Mehrotra. Asha, *GSM System Engineering*, Artech House Inc, Norwood, 1997

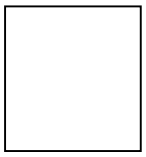
[6] Mehrotra. Asha, *Cellular Radio Analog and Digital System*, Artech House Inc, Norwood, 1994

[7] Mouly. Michael & Pautet. Marie-Bernandette, *The GSM System for Mobile Communication*, Michael Mouly & Marie-B Pautet Inc, France, 1992

[8] Schinier. Bruce, *Applied Cryptography*, 2nd edition, John Wiley & Sons, New York, 1996

[9] Sklar. Benard, *Digital Communication Fundamentals and Application*, Prentice Hall, New Jersey, 1988

[10] ....., *Signalling*, Training Section Satelindo, Jakarta, 1997



M Riza Miharja Tanjung, Lahir di Jakarta 24 tahun lalu, Mahasiswa Teknik Elektro UNDIP Angkatan '97 konsentrasi Telekomunikasi

Mengetahui:

Pembimbing I	Pembimbing II
Wahyudi,ST,MT	Achmad Hidayatno, ST,MT
NIP. 132086662	NIP. 132137933