Perbandingan Security Antara GSM dan CDMA

Rifky Hamdani / 13508024
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18024@students.if.itb.ac.id

***Abstract*— GSM (*Global System for Mobile Communication*) merupakan sistem yang paling banyak dipakai dalam komunikasi mobile. Sedangkan CDMA merupakan sistem lain yang dipakai dalam komunikasi mobile. Dalam makalah ini akan dibahas tentang pada GSM dan CDMA baik pada arsitektur dan *security*-nya.**

***Kata Kunci*—GSM, CDMA, Security**

I. PENDAHULUAN

Pada tahun 80an banyak sistem telekomunikasi analog yang digunakan di Eropa, seperti TACS (Total Access Communication System), NMT (Nordic Mobile Telephony), C-Netz, Radiocom-2000 dan varian yang lain. Oleh karena itu, pengguna hanya eksklusif terhadap operator tertentu dan tidak dapat berhubungan antar operator. Uni eropa membuat grup bernama *Group for Mobile Telephony* (GSM) mencoba untuk menyelesaikan masalah itu dengan membuat standar yang baru. Kemudian dibuatlah standar baru yang bernama GSM yang diikuti oleh sebagian besar operator di eropa.

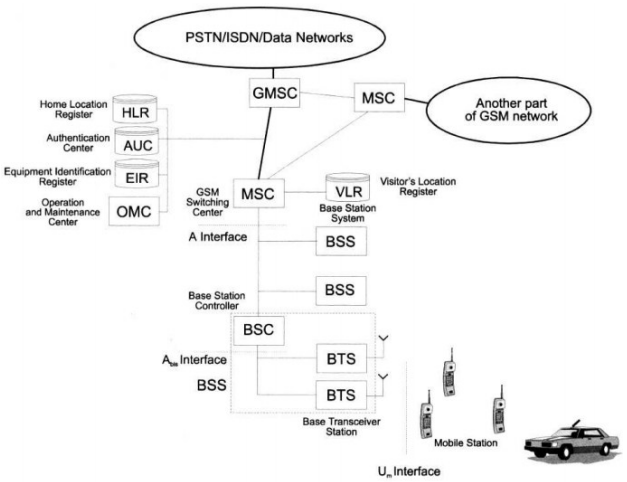
Code Division Multiple Access (CDMA) is adalah sebuah konsep radikal pada komunikasi nirkabel. Dengan konsep ini akan meningkatkan kapasitas dan kualitas layanan. Teknologi ini sendiri sudah ada sejak perang dunia II, tetapi baru digunakan pada akhir-akhir ini. Amerika merupakan negara yang memopulerkan teknologi ini. Teknologi ini berbasis pada multiakses dengan menggunakan kode.

II. GSM

A. GSM

Area operasi pada GSM dibagi menjadi beberapa sub area yang di atur oleh Mobile Switching Centers (MSC). MSC adalah switch elektronik yang memiliki block fungsional yang berfungsi untuk menyelesaikan tugas spesifik untuk sistem mobile seluler. Tiap MSC terhubung dengan basis data VLR (Visitor's Location Register). VLR berisi informasi sementara yang dibutuhkan untuk menjalankan sistem selular terkait telepon bergerak yang berada pada daerah MSC tersebut. Selain VLR, GSM memiliki basis data lain yang memiliki fungsi masing-masing yang berbeda dengan VLR.

HLR (Home Location Register), basis data dari telepon selular yang terdaftar secara permanen pada sistem administrasi oleh operator tertentu.
AUC (Authentication Center), basis data yang memungkinkan pengecekan pengguna dengan kartu SIM (Subscriber Identity Module) diperbolehkan untuk melakukan panggilan.
EIR (Equipment Identification Register), basis data yang berisi nomor seri dari telepon selular yang digunakan oleh sistem. Telepon yang hilang atau dicuri dapat dicegah untuk digunakan dalam sistem.



Gambar 1. Arsetektur GSM

HLR adalah database sentral yang menyimpan parameter permanen dari pengguna dan informasi di lokasi mereka saat ini. Dalam sistem yang besar bisa ada lebih dari satu HLR. Namun, data pengguna individu disimpan hanya dalam satu dari mereka. Register HLR berisi semua data pada pengguna secara permanen terdaftar di jaringan GSM, yang memungkinkan sistem untuk membangun jalur koneksi ke mereka, bahkan jika pada saat koneksi mereka sementara terdaftar dalam jaringan GSM yang berbeda dioperasikan di negara lain. Dengan demikian, catatan pengguna di HLR berisi status, *Temporary Mobile Identification Number* (TMSI) dan alamat dari register VLR yang berhubungan dengan area lokasi saat pengguna. Di antara data yang disimpan untuk setiap

pengguna, ada daftar layanan tambahan dipesan dan kunci enkripsi untuk transmisi sinyal digital dan otentikasi pengguna.

VLR adalah database terdiri dari catatan yang menjelaskan telepon selular saat ini terdaftar dalam jangkauan layanan MSC tertentu. VLR dan HLR register pertukaran data tentang pengguna saat ini berada di wilayah yang dilayani oleh VLR itu. Seperti pertukaran pengaturan dan informasi memungkinkan untuk identifikasi lokasi yang saat ini pengguna disebut dengan membaca informasi pada daerah lokasi saat nya di HLR dan routing koneksi ke MSC yang coworks dengan VLR saat ini berisi data pada pengguna yang disebut . Register VLR juga menyimpan data yang diperlukan untuk memulai panggilan.

Mobile Switching Center (MSC) terhubung satu sama lain. Satu atau lebih MCSs, disebut *Gateway Mobile Switching Center* (GMSC), memainkan peran sebagai gerbang ke jaringan eksternal seperti PSTN, ISDN dan jaringan data paket. Setiap MSC mengontrol setidaknya satu *Base Sistem Station* (BSS) yang terdiri dari *Base Station Controller* (BSC) dan sejumlah menara BTS (BTS) atau *base station* (BS). Base station terdiri dari subsistem melakukan transmisi sinyal pokok dan fungsi penerimaan sinyal dan unit melakukan fungsi kontrol sederhana. GSM-spesifik coding/decoding serta adaptasi data rate dilakukan di sini juga. Base station biasanya terletak di pusat sel-sel yang mencakup wilayah sistem operasi keseluruhan. Dalam sel-sel tersebut, sejumlah Mobile Stations (MS) beroperasi dengan kemungkinan perubahan lokasi mereka secara dinamis. Mereka melakukan pertukaran informasi dengan yang paling dekat (atau yang terkuat pada titik lokasi) base station.

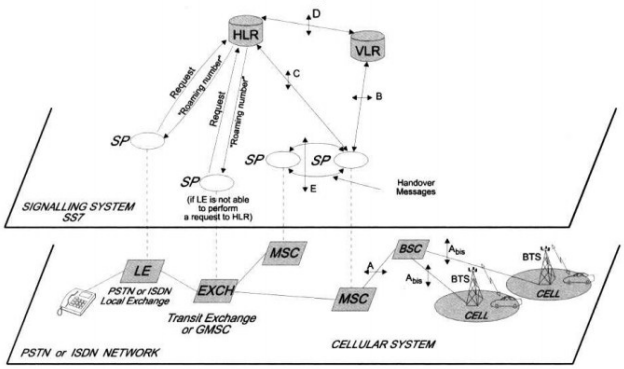
Tugas utama dari MSC adalah mengkoordinasikan panggilan set-up antara dua pengguna GSM atau antara pengguna GSM dan pengguna dari jaringan eksternal seperti PSTN, ISDN atau PSDN (*Public Switched Data Network*).

Pertukaran informasi antara MSC dan BSS dinormalkan dengan mendefinisikan apa yang disebut antarmuka A, sedangkan antarmuka Abis standarisasi pertukaran data antara controller dan transceiver base station-nya (BTS).

Antarmuka yang kebanyakan berhubungan dengan jaringan dan aspek switching, misalnya dengan fungsi yang dilakukan oleh MSC, HLR dan VLR, dengan manajemen link tetap, dengan manajemen jaringan, mengendalikan dan enkripsi data pengguna dan sinyal informasi, dengan manajemen yang dihasilkan dari perlunya otentikasi MS dan meng-update lokasi yang disebabkan oleh gerakan MS geografis dan dengan manajemen pengguna telepon.

Antarmuka Abis berhubungan dengan pertukaran informasi yang berhubungan dengan transmisi radio, seperti distribusi saluran radio, koneksi mengawasi, antrian pesan sebelum transmisi, frekuensi pembawa hopping kontrol (Frequency Hopping FH), jika diterapkan, saluran coding dan decoding, coding dan decoding dari sinyal suara, enkripsi pesan dan memancarkan power control.

Operation and Maintenance Center (OMC) mengawasi pengoperasian blok sistem GSM tertentu. Hal ini terhubung dengan semua blok beralih dari sistem GSM dan melakukan fungsi manajemen seperti akuntansi tarif, pemantauan lalu lintas, manajemen dalam hal kegagalan blok jaringan tertentu. Salah satu tugas paling penting dari OMC adalah HLR manajemen. Dalam hal jaringan besar ada lebih dari satu OMC dan seluruh jaringan dikelola oleh *Network Management Center* (NMC). Komunikasi antara OMC dan blok jaringan direalisasikan oleh manajemen jaringan komunikasi khusus dilaksanakan dengan link telepon disewakan atau jaringan tetap lainnya. Transfer pesan dilakukan menggunakan protokol signaling SS7 dan X.25 protokol untuk interface A dan Abis.



Gambar 2. Arsitektur basis data pada GSM

B. Security pada GSM

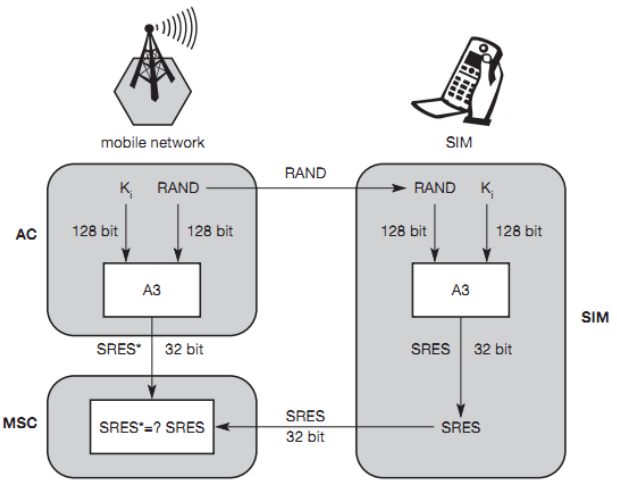
GSM memberikan beberapa layanan securiti menggunakan informasi yang confidensial yang di simpan di AuC dan pada tiap kartu SIM. Kartu SIM menyimpan data rahasia dengan PIN untuk mencegah penyalahgunaan. Layanan keamanan yang ditawarkan yaitu:

- Access control and authentication: Langkah pertama berisi otentikasi dari pengguna SIM. Pengguna membutuhkan PIN untuk mengakses SIM. Langkah selanjutnya adalah otentikasi pengguna
- Confidentiality: Semua data yang berkaitan dengan pengguna dienkripsi. Setelah diotentikasi BTS dan MS melakukan enkripsi pada data, suara dan signal. Kerahasiaan hanya terjadi antara MS dan BTS.
- Anonymity: Untuk menyediakan anonimitas pada pengguna semua data dienkripsi sebelum ditransmisikan

Tiga algoritma telah ditetapkan untuk memberikan layanan keamanan dalam jaringan GSM. Algoritma A3 digunakan untuk otentikasi, A5 untuk enkripsi, dan A8

untuk generasi kunci cipher. Dalam algoritma standar GSM A5 adalah hanya tersedia untuk publik, sedangkan A3 dan A8 adalah rahasia, tapi standar dengan antarmuka terbuka. Kedua A3 dan A8 tidak lagi rahasia, tapi dipublikasikan di internet pada tahun 1998. Ini menunjukkan bahwa keamanan dengan ketidakjelasan tidak benar-benar bekerja. Ternyata, algoritma tidak sangat kuat. Namun, penyedia jaringan dapat menggunakan algoritma yang lebih kuat untuk otentikasi - atau pengguna dapat menerapkan kuat end-to-end enkripsi. Algoritma A3 dan A8 (atau pengganti mereka) terletak di SIM dan dalam AUC dan dapat proprietary. A5 Hanya yang diimplementasikan dalam perangkat harus identik untuk semua provider.

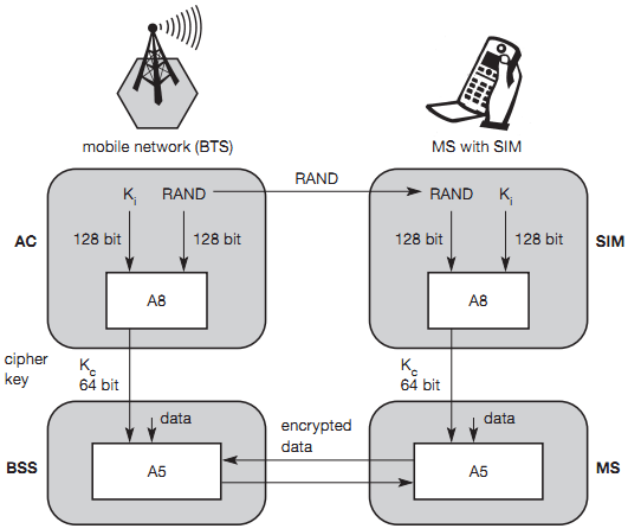
Authentication. Sebelum pelanggan bisa menggunakan layanan apapun dari jaringan GSM, ia harus disahkan. Otentikasi didasarkan pada SIM, yang menyimpan Ki otentikasi kunci individu, pengguna IMSI identifikasi, dan algoritma A3 digunakan untuk otentikasi. Otentikasi menggunakan metode tantangan-respon: Akses kontrol AC menghasilkan angka acak RAND sebagai tantangan, dan SIM dalam jawaban MS dengan SRES (respon ditandatangani) sebagai respon (lihat Gambar 4.14). Para AUC melakukan generasi dasar nilai acak RAND, SRES ditandatangani tanggapan, dan kunci cipher Kc untuk IMSI masing-masing, dan kemudian meneruskan informasi ini ke HLR. Permintaan VLR saat ini yang sesuai nilai untuk RAND, SRES, dan Kc dari HLR.



Gambar 3. Enkripsi pada GSM

Untuk otentikasi, VLR mengirimkan RAND nilai acak ke SIM. Kedua belah pihak, jaringan dan modul pelanggan, melakukan operasi yang sama dengan RAND dan Ki kunci, disebut A3. MS mengirimkan kembali SRES dihasilkan oleh SIM; VLR sekarang dapat membandingkan kedua nilai-nilai. Jika mereka adalah sama, VLR menerima pelanggan, jika pelanggan ditolak.

Encryption. Untuk memastikan privasi, semua pesan yang berisi informasi pengguna yang berhubungan akan dienkripsi dalam jaringan GSM melalui antarmuka udara. Setelah otentikasi, MS dan BSS dapat mulai menggunakan enkripsi dengan menggunakan kunci cipher Kc (lokasi yang tepat dari fungsi keamanan untuk enkripsi, BTS dan / atau BSC adalah vendor yang tergantung). Kc dihasilkan menggunakan Ki kunci individual dan nilai acak dengan menerapkan algoritma A8. Perhatikan bahwa SIM pada MS dan jaringan baik menghitung Kc yang sama berdasarkan nilai acak RAND. Kc kunci itu sendiri tidak ditularkan melalui antarmuka udara.



Gambar 4. Enkripsi pada GSM

MS dan BTS sekarang dapat mengenkripsi dan mendekripsi data menggunakan algoritma A5 dan Kc cipher kunci. Kc harus menjadi kunci 64 bit - yang tidak sangat kuat, tapi setidaknya perlindungan yang baik terhadap menguping sederhana. Namun, penerbitan A3 dan A8 di internet menunjukkan bahwa dalam implementasi tertentu 10 dari 64 bit selalu set ke 0, sehingga panjang sebenarnya kuncinya adalah dengan demikian hanya 54 akibatnya, enkripsi ini jauh lebih lemah.

III. CDMA

A. CDMA

Pada GSM digunakan skema FDMA and TDMA *access schemes*. Dalam beberapa tahun terakhir Code Division Multiple Access (CDMA) adalah fokus perhatian pusat penelitian industri dan akademis, sehingga pembangunan yang besar dalam komunikasi akses jamak menggunakan teknik spread spectrum dengan urutan menyebarkan individu diterapkan oleh pengguna. Saat ini, CDMA adalah metode yang mendominasi akses ganda dalam generasi ketiga (3G) sistem komunikasi mobile. Sebagian besar proposal IMT-2000 (International Mobile Telecommunications) keluarga standar International Telecommunication Union (ITU) mengandalkan CDMA

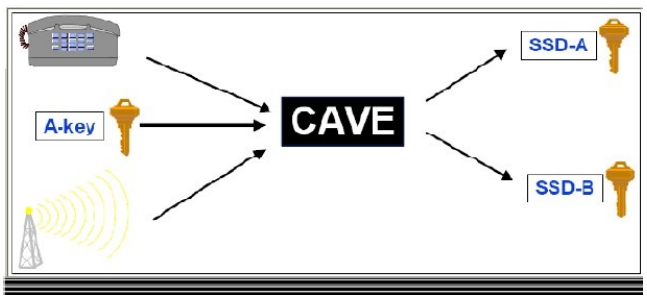
sebagai beberapa metode akses.

B. Security pada CDMA

Sejak kelahiran industri seluler, keamanan telah menjadi perhatian utama bagi penyedia layanan dan penyedia subscribers. Service terutama prihatin dengan keamanan untuk mencegah operasi penipuan seperti kloning atau penipuan berlangganan, sementara pelanggan terutama peduli dengan masalah privasi. Pada tahun 1996, kegiatan penipuan throughcloning dan operator biaya lain berarti sekitar US $ 750 juta pendapatan yang hilang di Amerika Serikat saja. Penipuan adalah masalah stilla hari ini, dan IDC memperkirakan bahwa pada tahun 2000, operator kehilangan lebih dari US $ 180 juta dalam pendapatan dari penipuan fraud.Technical, seperti kloning, menurun di Amerika Serikat, sedangkan penipuan berlangganan adalah pada rise1 tersebut. Dalam tulisan ini, kita akan membatasi diskusi kita untuk penipuan teknis saja. Dengan munculnya generasi kedua platform teknologi digital seperti TDMA/CDMA-IS-41, operator mampu meningkatkan keamanan jaringan mereka dengan menggunakan algoritma improvedencryption dan sarana lainnya. Tanda tangan suara seperti dari sinyal CDMA selama makeseavesdropping antarmuka udara sangat sulit. Hal ini disebabkan "Long Code," CDMA 42-bit PN (Pseudo-Random Kebisingan dari length242-1) urutan, yang digunakan untuk berebut suara dan transmisi data. Makalah ini membahas bagaimana CDMA 20001xRTT mengimplementasikan tiga fitur utama dari keamanan mobile: otentikasi, perlindungan data, dan anonimitas

Security – CDMA Networks

Protokol keamanan dengan jaringan CDMA-IS-41 adalah yang terbaik di industri. Dengan desain, teknologi CDMA membuat penyadapan sangat sulit, baik disengaja atau tidak disengaja. Unik untuk sistem CDMA, adalah 42-bit PN (Pseudo-Random Noise) Urutan disebut "Long Code" untuk men-*scrable* suara dan data. Pada forward link (jaringan tomobile), data di-*scrable* pada rate 19.2 Kilo simbol per detik (Ksps) dan pada reverse link, data diperebutkan tingkat ata dari 1.2288 Mega chips per detik (Mcps). CDMA keamanan jaringan protokol mengandalkan otentikasi kunci 64-bit (A-Key) dan Nomor Seri Elektronik (ESN) dari mobile.



Gambar 5. Kunci pada CDMA

Sejumlah bilangan acak yang disebut RANDSSD, yang dihasilkan di HLR / AC, juga menjalankan peran dalam prosedur authentication. The A-Key diprogram dalam mobile dan disimpan dalam Authentication Center (AC) dari penambahan network.In untuk otentikasi, A-Key digunakan untuk membangkitkan sub-key untuk privacy suara dan pesan encryption.CDMA menggunakan CAVE standar (Cellular Authentication dan Voice Encryption) algoritma untuk menghasilkan 128-bitsub-kunci yang disebut "Data Rahasia bersama" (SSD). A-Key, ESN dan jaringan yang dipasok RANDSSD adalah masukan ke CAVE yang menghasilkan SSD. SSD memiliki dua bagian: SSD_A (64 bit), untuk membuat otentikasi signaturesand SSD_B (64 bit), untuk membangkitkan kunci untuk encrypt pesan suara dan sinyal. SSD dapat di share dengan penyedia roaming service untuk memungkinkan local authentication. SSD yang baru dapat digenerate ketika mobile kembali ke home network atau roam ke sistem yang berbeda.

Authentication

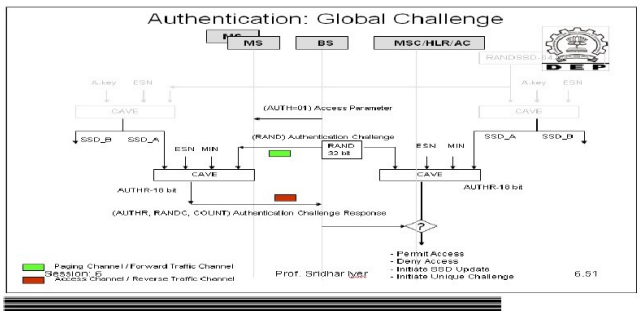
Dalam jaringan CDMA, mobile menggunakan SSD_A dan *broadcast* RAND * sebagai input terhadap algoritma CAVE togenerate tanda tangan 18-bit otentikasi (AUTH_SIGNATURE), dan mengirimkannya ke base station. Ini isthen tanda tangan digunakan oleh base station untuk memverifikasi bahwa subscriber tersebut sah. Kedua Global Challenge (dimana semua ponsel arechallenged dengan nomor acak yang sama) dan Tantangan unik (dimana spesifik RAND digunakan untuk setiap requestingmobile) prosedur yang tersedia untuk para operator untuk otentikasi. Metode Global Challenge memungkinkan sangat rapidauthentication. Juga, baik mobile dan track jaringan Call History Count (6-counter bit). Ini menyediakan diri untuk mendeteksi kloning, sebagai operator akan diberitahu jika ada mismatch.The Kunci-adalah kembali diprogram, namun kedua themobile dan Pusat Otentikasi jaringan

Basic of authentication :

ESN (*electronic serial number*) adalah 32-bit *serial number* elektronik dari ponsel. ESN adalah pra-diprogram oleh phonemanufacturer selama pengaturan pabrik. ESN adalah unik untuk setiap ponsel di jaringan dan digunakan dalam jumlah hubungannya withthe mobile untuk identitas mobile pada jaringan. MIN (nomor identifikasi mobile) MIN adalah 10 digit angka yang diberikan oleh penyedia layanan untuk ponsel dalam jaringan. Minis yang unik setiap ponsel di jaringan dan digunakan dalam hubungannya dengan ESN untuk mengidentifikasi mobile di network. MDN (Mobile directory number) MDN adalah nomor 10 digit yg dpt dibesarkan diberikan oleh penyedia layanan untuk telepon amobil pada jaringan. MDN mungkin sama dengan MIN (itu tergantung pada bagaimana penyedia layanan provisionsthis pasangan pada jaringan).

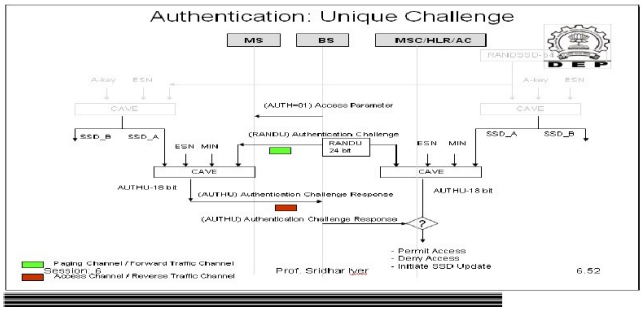
Global challenge
Global challenge dilakukan ketika:

- Registration
- Origination
- Terminations
- Mobile station data



Gambar 6. Otentikasi pada CDMA

Unique Challenge
sinyal MS ditantang dengan nomor acak yang dipilih (unik) VLR dapat memulai SSD jika dibagi (hanya laporan toAC kegagalan) dapat dijalankan pada saluran lalu lintas digunakan untuk panggilan menghemat kontrol saluran resourcesBy desain, semua ponsel CDMA menggunakan PN unik (Pseudo-random Noise) kode untuk Menyebarkan thesignal, yang membuat sulit bagi sinyal yang akan disadap.



Gambar 7. Otentikasi pada CDMA

The inherent security of the CDMA air interface
Code Division Multiple Access (CDMA) adalah teknologi nirkabel yang luas untuk suara dan kecepatan tinggi akses internet kecepatan mendukung mobilitas tinggi. CDMA secara inheren aman dan memiliki kelebihan untuk generasi pertama analog dan Time Division Access sistem (TDMA) Berganda. CDMA berasal dari kriptografi militer dan data tidak pernah ada laporan dari pembajakan tinggi atau penyadapan panggilan CDMA di jaringan non komersial. Keamanan yang melekat pada interface udara CDMA berasal dari kombinasi enkripsi dan teknologi spread spectrum, yang digunakan secara bersamaan untuk membatalkan setiap celah keamanan. CDMA sinyal dari semua panggilan dikirim atau tersebar di seluruh bandwidth bukannya terikat dengan elemen tertentu timeor dalam sistem. ini mengakibatkan sinyal dari semua panggilan penyambungan white noise penampilan kebisingan-seperti yang bekerja sebagai menyamarkan membuat sinyal dari setiap panggilan satu sulit untuk membedakan dan mendeteksi dari *noise* latar belakang

IV. PERBANDINGAN GSM DAN CDMA

A. Perbandingan Umum

GSM mengaharuskan memiliki jumlah BTS tertentu tiap jumlah pengguna sehingga dapat dijaga kualitas yang diberikan.

CDMA tidak mengharuskan memiliki jumlah BTS tertentu tiap user. Sinyal akan terus ditambah kodenya apabila ada pengguna baru yang masuk pada BTS. Sehingga semakin banyak pengguna yang masuk maka kualitas yang ada akan menurun. Selain itu pada pengguna yang jauh dari BTS akan terjadi penurunan kualitas yang sangat banyak.

B. Perbandingan Security

GSM tidak menggunakan skema multiakses pada kode karena itu GSM rentan terhadap penyadapan karena GSM hanya menggunakan TDMA(Time Division Multiple Acces) dan FDMA (Frequency Division Multiple Acces).

CDMA menggunakan multiakses dengan kode oleh karena itu sangat sulit untuk melakukan penyadapan pada CDMA. Apabila kita melakukan penyadapan pada CDMA dan tidak memiliki kunci maka kita hanya akan mendapatkan sinyal noise. Hal itu dapat terjadi karena pada CDMA sinyal beberapa user digabungkan menjadi satu saat *broadcast* kemudian di decripsi dengan kunci-kunci tertentu pada tiap pengguna sehingga pengguna hanya mendapatkan sinyal yang seharusnya dia terima

V. KESIMPULAN

Dari hasil keterangan di atas dapat ditarik kesimpulan bahwa:

- ❖ CDMA memiliki keamanan yang lebih baik dari pada GSM karena memiliki
- ❖ Kualitas layanan GSM lebih baik daripada CDMA karena semakin jauh pengguna dari BTS layanan CDMA akan semakin buruk

REFERENSI

[1] J. Schiller, "Mobile Communication 2nd Ed," Harlow: Pearson Education Limited, 2003.

[2] K. Wesolowski, "Mobile Communication System," West Sussex: John Wiley & Son, 2002

[3] http://en.wikipedia.org/wiki/GSM (diakses pada tanggal 7 Mei 2012).

[4] http://en.wikipedia.org/wiki/Code_division_multiple_access (diakses pada tanggal 7 Mei 2012)

[5] http://en.wikipedia.org/wiki/IS-95 (diakses pada tanggal 7 Mei 2012)

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 12 Mei 2012

Rifky Hamdani / 13508024