Sekuritas Sinyal *Voice/Data* pada Sistem GSM

Hidajanto Djamal
Dosen Fakultas Teknik Universitas Mercu Buana
Jl Meruya Hilir Jakarta
hidajanto_djamal@yahoo.com

Abstract

Dalam beberapa pemberitaan di surat kabar belakangan ini mengatakan bahwa, penyadapan berhasil dilakukan pada pembicaraan telepon seluler GSM oleh yang berwajib. Ini menunjukkan bahwa, sistem GSM tidak mempunyai sekuritas yang cukup. Apakah memang demikian ? Uraian dalam paper kajian ini akan menunjukkan hal yang sebaliknya, yaitu, 'perlindungan' terhadap voice/data dilakukan berlapis dalam sistem GSM. Keberhasilan penyadapan tentu saja dapat dilakukan dengan satu rekayasa teknik yang dilakukan vendor sendiri untuk keperluan tertentu atas permintaan institusi yang mempunyai legalitas.

Katakunci : GSM, perlindungan data

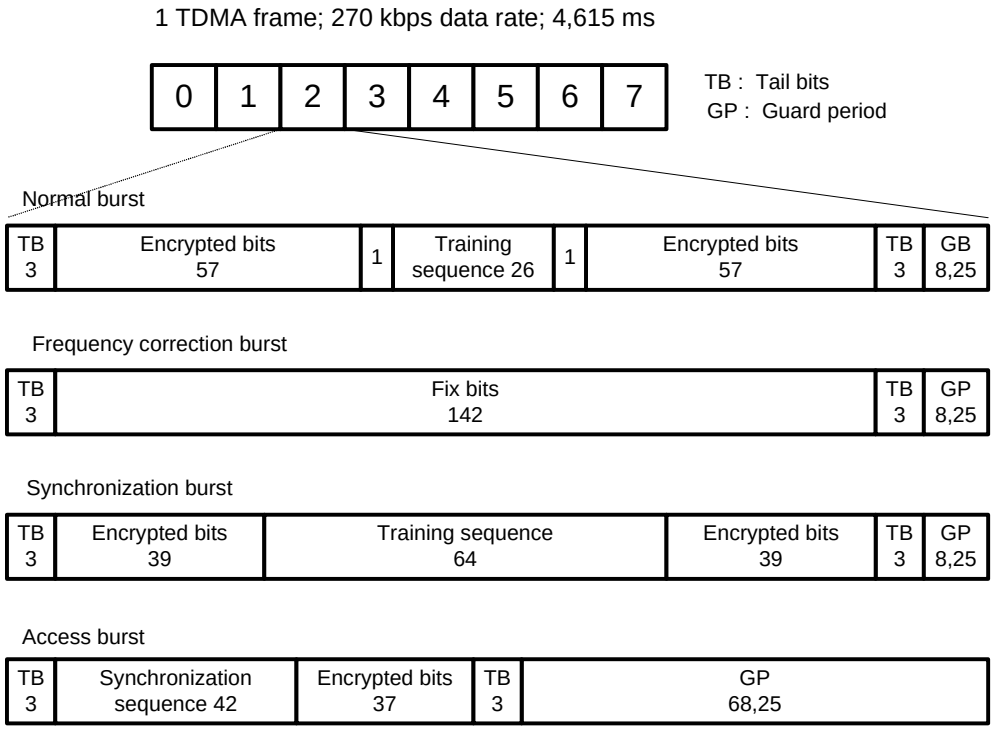
1. Pendahuluan

Pengiriman sinyal informasi dengan menggunakan satu frekuensi radio (RF = radio Frequency) ke udara yang tentunya menggunakan satu sistem antena, dapat dilakukan bila menggunakan proses modulasi. Termasuk informasi disini, adalah sinyal voice dan juga data pada sistem telepon seluler. Sinyal informasi dimodulasikan pada sinyal dengan frekuensi RF, yang dalam hal sistem GSM, frekuensi RF tersebut berada pada pita 900 MHz, atau 1800 MHz untuk sistem DCS, atau pada pita 800 MHz untuk sistem CDMA.

Sinyal voice maupun data adalah sinyal dalam bentuk digital, sehingga modulasi yang diterapkan adalah modulasi digital (bukan modulasi analog seperti AM = amplitude modulation, atau FM = frequency modulation). Jenis modulasinya adalah PSK (phase shift keying) dalam beberapa versinya, seperti QPSK (quadrature phase shift keying), atau versi FSK (frequency shift keying). Pada sistem GSM, modulasi pulsa yang diterapkan adalah FSK yang diimplementasikan pada modulasi GMSK (Gaussian Minimum Shift Keying).

1.1 Format Sinyal Digital dalam Time Slot

Karena pengiriman sinyal informasi tersebut dalam beberapa kanal, maka harus dilakukan dengan jalan teknik pemberkasan. Pemberkasan kanal dilakukan secara FDMA dan TDMA, baik untuk jalur *uplink* maupun *downlink*. Dengan FDMA dihasilkan 124 pasang kanal yang disebut dengan *superchannel*, yang kemudian pada masing-masing kanal tersebut, dilakukan proses TDMA sehingga dihasilkan 8 pasang kanal untuk arah *uplink* dan *downlink* tersebut. Oleh karena itu masing-masing kanal frekuensi tersebut dinamakan *TDMA frame* seperti ditunjukkan pada Gbr-1.



Gambar 1 Format *frame time slot* TDMA pada system GSM

Selanjutnya, masing-masing dari delapan kanal itu yang dinamakan *traffic channel* (TCH) merupakan pasangan kanal untuk satu MS yang berkomunikasi dengan satu BTS. Jadi satu kanal dalam sistem GSM adalah satu celah waktu (*time slot*) yang berulang untuk setiap *TDMA frame* dengan satu frekuensi pancaran tertentu dalam satu arah, *uplink* atau *downlink*. Karena satu pasang, maka terdapat satu *time slot* yang lain yang berulang untuk setiap frame pada frekuensi pancaran yang lain untuk arah sebaliknya.

TDMA frame yang dimaksudkan diatas mempunyai total bit rate sebesar 270 kbps, terbagi dalam 8 *time slot* dan mempunyai durasi sebesar 4,615 milisekon seperti ditunjukkan pada Gbr-1 di atas. Masing-masing *time slot* dapat difungsikan sebagai *traffic channel* seluruhnya, atau dua diantaranya digunakan sebagai *dedicated channel* guna pengaturan akses bagi MS. *Dedicated channel* itu adalah SDCCH dan BCCH yang biasanya menempati TS_0 dan TS_1 untuk masing-masing frekuensi. Bila satu BTS bekerja sebagai pemancar sektoral dan mengoperasikan lebih dari satu TRX dalam satu sektor, maka *dedicated channel* tersebut berada pada satu frekuensi, sementara frekuensi kerja yang lain diatur seluruh delapan *time slot* nya berfungsi sebagai TCH. *Traffic channel* yang tersedia itu dapat diakses oleh setiap MS yang beroperasi pada frekuensi tersebut.

Pada Gbr-1 nampak, bahwa masing-masing *time slot* yang dimasudkan mempunyai kemungkinan berbentuk salah satu dari empat format frame atau *burst*, yaitu; *normal burst*, *frequency correction burst*, *synchronization burst*, atau *access burst* yang bergan-tung pada mode proses yang sedang berlangsung.

Bentuk yang umum dari keempat burst tersebut adalah *normal burst* yang digunakan pada saat berlangsung hubungan telepon, dimana pensinyalan SACCH (*slow associated control channel*) dan FACCH (*fast associated control channel*) berada. Kanal pembica-raan/data terletak pada slot *encrypted bits*. Pensinyalan FACCH tidak

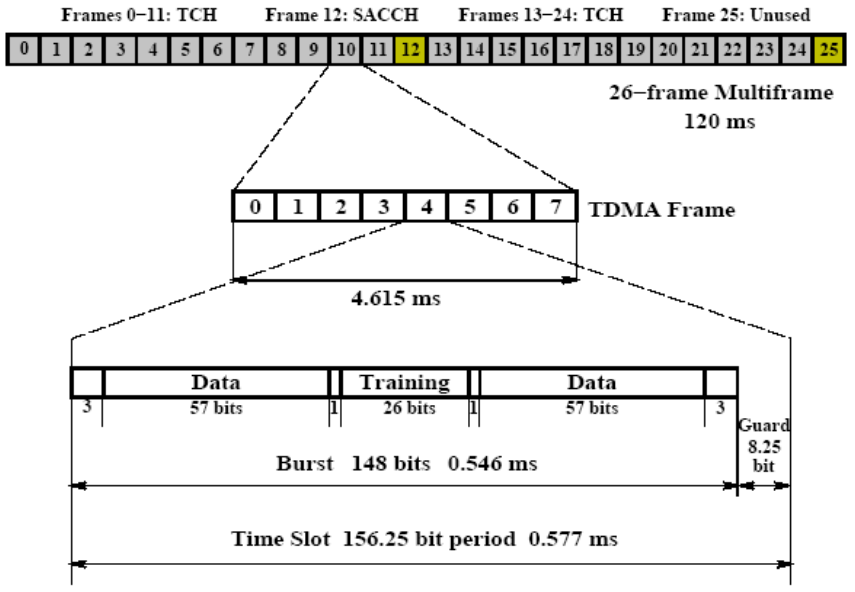
lain adalah kanal SDCCH dan BCCH yang diatur menempati slot TS_0 dan TS_1. Kanal ini dapat juga digunakan untuk mengirim *short message services* (SMS). Kanal ini juga yang diguna-kan untuk proses *authentication*, yang akan dibahas kemudian. Proses otentikasi terjadi pada satu MS yang baru masuk dalam wilayah layanan satu BTS tertentu.

Sedang *frequency correction burst*, digunakan oleh BS untuk melakukan koreksi frekuensi kanal (*fine-tuning*) yang digunakan MS. Sementara *synchronization burst*, digunakan untuk melakukan sinkronisasi detak (*clock*) antara MS dengan BS atau sebaliknya yang dimungkinkan dengan adanya *training sequence* yang ditempatkan di tengah-tengah frame untuk memberi pengaruh efektif sinkronisasi pada seluruh frame. Sedang a*ccess burst*, digunakan MS untuk meminta kanal kepada BS.

Ketika satu MS meminta kanal kepada BS melalui *access burst*, dan saat itu kebetulan tepat bersamaan dengan MS yang lain yang sedang meminta kanal, maka MS terakhir tersebut menunggu dalam beberapa saat dan mencoba kembali. Hal ini mirip dengan cara kerja protokol pada sistem LAN.

Pada *normal-burst* maupun *synchronization-burst* terdapat *training-sequence* yang ditempatkan di tengah-tengah frame untuk memberikan pengaruh efektif sinkronisasi pada seluruh frame. Juga pada setiap jenis burst diatas terdapat *tail bits* (TB) dan *guard period* (GP). *Guard period* digunakan untuk memberi kompensasi kesalahan dalam keakuratan sinkronisasi detak, dan kompensasi perbedaan jarak beberapa lokasi MS terhadap BS. Sedang TB digunakan sebagai tanda awal dan akhir data pada masing-masing format burst.

TDMA frame yang ditunjukkan pada Gbr-1, akan berulang dalam siklus waktu, yang merupakan bagian dari multiframe. Multiframe yang dimaksudkan ditunjukkan pada Gbr-2 yang terdiri dari 26 TDMA frame dengan siklus 120 ms. Dari Gbr-1 nampak, bahwa satu time-slot akan menampung data (*voice* digital atau data) dengan bit-rate sampai 33,75 kbps.



Gambar 2 Format frame TDMA pada multiframe system GSM

Pada Gbr-2 nampak, bahwa dari 26 frame tersebut, 24 frame digunakan sebagai TDMA frame yang berisi TCH. Satu frame, yaitu frame-25 tidak digunakan, sementara frame-12 digunakan untuk pensinyalan SACCH (*slow associated control channel*).

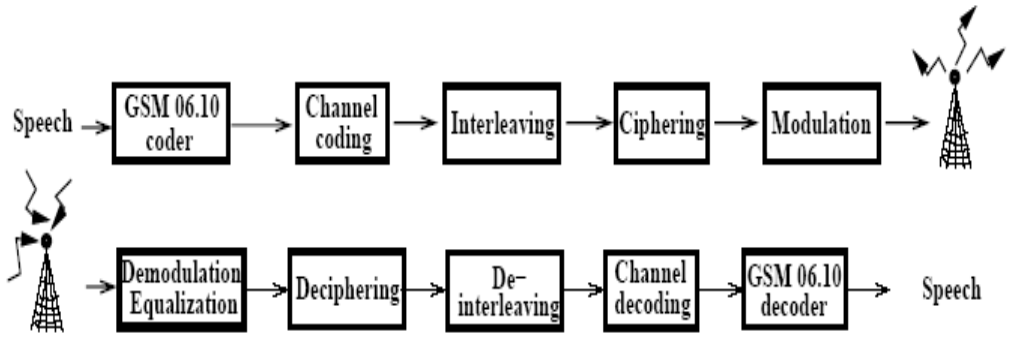
Pensinyalan SACCH digunakan terutama untuk mengirimkan data pengukuran level pancaran dalam proses keputusan *handoff*, yang dikirimkan per detik sebanyak dua pesan untuk setiap MS.

1.2 Bukti Sekuritas Voice/Data

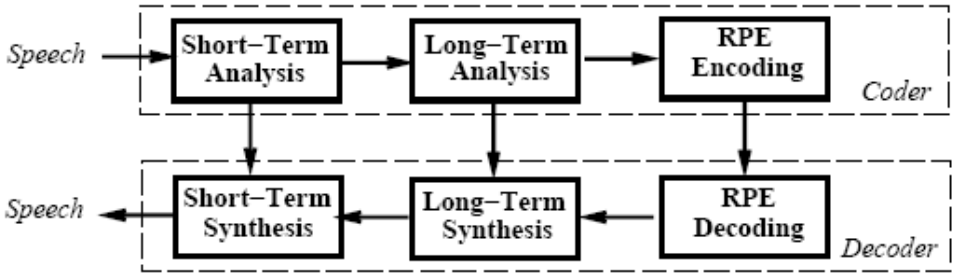
Dari sederetan bit (bit stream) yang membawa informasi data pada sistem GSM seperti ditunjukkan pada Gbr-1, terutama untuk *normal burst* yang digunakan pada saat berlangsung mode pembicaraan, nampak memberikan gambaran bahwa sinyal voice/data tersebut berada pada dereten yang teracak di kiri dan kanan sederetan bit-bit untuk sinkronisasi frame (*training sequence*). Proses pengacakan atau pengkodean tersebut melalui beberapa tahapan diantaranya adalah proses *convolution code,* sehingga voice/data itu berada pada kondisi sangat aman terhadap penyadapan. Tahapan proses dimaksud akan diuraikan berikut ini.

2. Pembahasan

Diagram blok yang menunjukkan proses pengolahan tersebut ditunjukkan pada Gbr-3 berikut ini, dimulai dari sinyal voice yang analog sampai ke proses modulasi yang disebut di atas sebagai sistem GMSK (*Gaussian Minimum Shift Keying*).



Gambar 3 Diagram blok proses dari *voice* ke *radio waves*



Gambar 4 Diagram blok proses pengolahan sinyal *voice*

Pada Gbr-3 ditunjukkan proses yang terjadi pada sisi MS atau hp yang kita gunakan, yaitu pada arah *upload* dan kemudian *download* yang merupakan proses sebaliknya. Proses dimulai dari proses *speech coding,* yaitu menjadikan sinyal *voice* analog menjadi sinyal dengan format digital.

2.1 Pengolahan sinyal *voice*

Sistem *coding* yang dilakukan dikenal sebagai RPE-LTP (Residual Pulse Excitation with Long Term Prediction) yang diberi

kode GSM 06.10 RPE-LTP pada awal rancangannya, dan melalui modifikasi menjadi versi kedua dengan kode GSM 06.20 RPE-LTP. Pada dasarnya, encoder memilah sinyal voice menjadi tiga kategori, yaitu, *short-term predictable parts*, *long-term predictable parts*, dan bagian yang tidak termasuk keduanya yang disebut sebagai *residual pulse*. Diagram blok sistem *codec* (*coder-decoder*) pengolahan sinyal voice tersebut ditunjukkan pada Gbr-4.

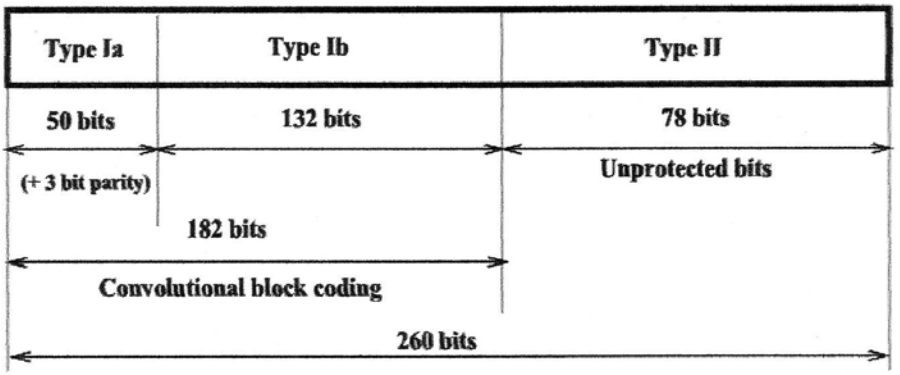
Pada Gbr-4 ditunjukkan kedua blok proses ini secara keseluruhan, yang pada Gbr-3 adalah blok GSM-06.10 *coder* pada sisi transmit, dan blok GSM-06.10 *decoder* pada arah receive. Pada arah terima, inputan yang masuk adalah melalui blok *RPE decoding*, yang dalam blok keseluruhan sistem (perhatikan Gbr-3) berasal dari blok *Channel decoding*. Hubungan yang digambarkan pada Gbr-4 antara blok padanannya adalah hubungan *logical* saja. Proses coding yang berlangsung bertumpu pada software yang dirancang untuk itu oleh peneliti Technical University of Berlin, ***Jutta Degener*** dan ***Carsten Bormann***. Sementara versi keduanya, GSM 06.20 RPE-LTP, dirancang untuk dapat bekerja dengan moda *half-rate speech encoding*.

Proses encoding dimulai dengan proses prediksi untuk masing-masing *term*, bagian *short* dan *long-term*, serta pengkodean pulsa-pulsa selebihnya. Kemudian pada sisi terima, proses decoding dimulai dengan men-decode residual pulse yang kemudian melewatkan ke filter *long-term* prediction. Selanjutnya, tahapan terakhir adalah ke filter *short-term*. Outputnya adalah sinyal voice kembali.

2.2 Pengkodean kanal

Pengkodean kanal adalah proses membentuk bit-stream baru dari bit-stream awal data, yaitu dengan menambah beberapa bit redundant untuk keperluan deteksi dan koreksi *error* yang mungkin terjadi selama ditransmisikan.

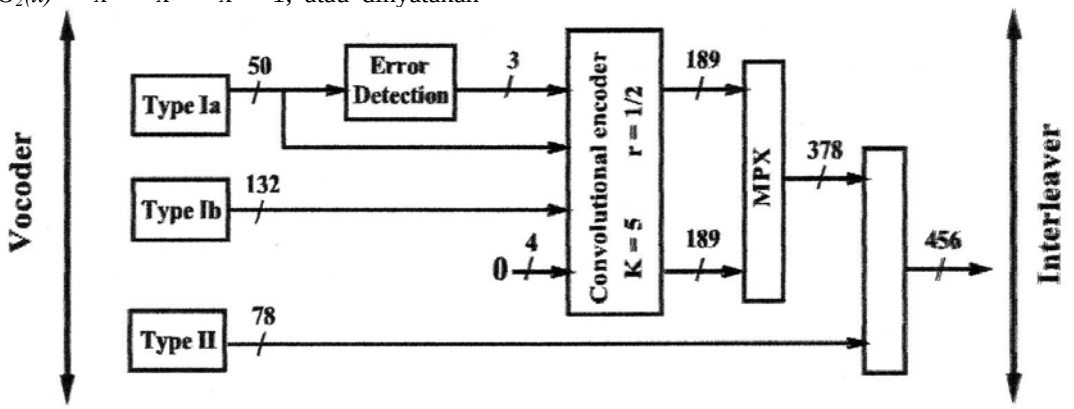
Dengan algoritma tertentu, dihasilkan satu blok data yang terdiri dari 260 bit untuk setiap 20 milisekon, yaitu sama dengan bit rate 13 kbps. Blok data tersebut kemudian dibagi ke dalam dua grup, grup-I dan grup-II. Pembagian blok 260 bit tersebut ditunjukkan pada Gbr-5. Grup-II yang terdiri dari 78 bit, diperuntukkan bagi bit-bit yang tidak begitu penting dan tidak diproteksi. Sementara grup-I yang terdiri dari 182 bit dibagi menjadi grup-Ia (50 bit) dan grup-Ib (132 bit).



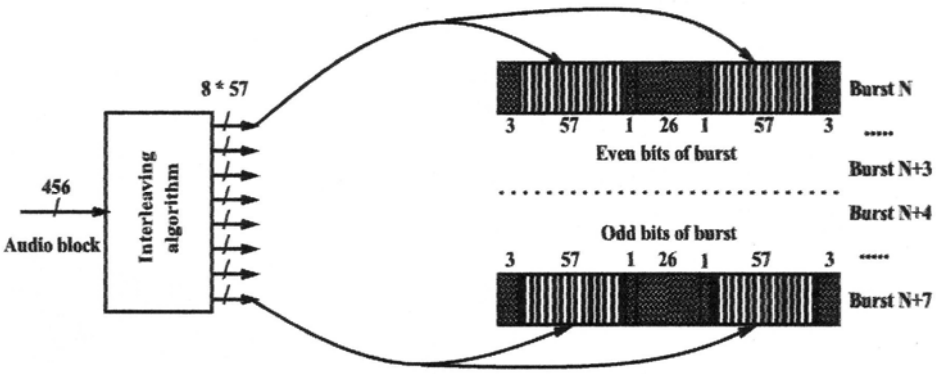
Gambar 5 Pembagian blok 260 bit menjadi dua grup

Selanjutnya, bit-bit grup atau type-Ia dilengkapi 3 bit tambahan untuk deteksi error. Setelah itu grup-Ia dan Ib yang ditambah 4 bit baru, dikodekan kembali (*convolutional encoding*) dengan *rate*, r = ½, dan *constraint length*, K = 5. Hasil pengkodean itu adalah 378 bit stream, yang kemudian ditambah bit-bit pada grup-II. Hasil terakhirnya adalah satu frame sinyal data suara yang terkode dengan jumlah bit seba-nyak 456 bit. Seluruh proses channel coding ditunjukkan pada Gbr-6.

Dalam blok convolutional-encoder terjadi proses pengkodean yang mengikuti algoritma tertentu, yaitu mengikuti dua fungsi polynomial, $G_1(x) = x^4 + x^3 + 1$, atau $(11001)_2$ dan menghasilkan satu output. Dan fungsi polynomial kedua adalah $G_2(x) = x^4 + x^3 + x + 1$, atau dinyatakan sebagai $(11011)_2$ dan menghasilkan output yang kedua. Hasil pengkodean dengan dua polynomial tersebut, masing-masing adalah 189 bit, yaitu, dari jumlah (185 bit + 5 bit – 1 bit). Lima bit berasal dari proses masing-masing generator polynomial tersebut.



Gambar 6 Proses pembentukan *bit-stream* sinyal suara (*voice*)



Gambar 7 Proses *interleaving sinyal audio-block*

Kedua sinyal digital 189 bit tersebut kemudian disisipkan secara bergantian satu sama lain seperti kalau kita menempatkan jari-jari kedua tangan antara satu dengan yang lain. Proses ini dilakukan oleh blok MPX yang merupakan *electronic-switch*. Electronic-switch ini bekerja dengan kecepatan detak 2 x laju bit kedua deretan bit 189 tersebut, sehingga menjadi 378 bit yang kemudian ditambah dengan 78 bit sinyal voice Type-II. Dengan penjumlahan tersebut, maka data tersebut akhirnya menjadi data dengan panjang frame 456 bit. Proses selanjutnya yang dialami adalah proses *interleaving*, yang merupakan blok ke-3 pada Gbr-3 di depan.

2.3 Proses *Interleaving*

Interleaving berarti membuat terpisah kelompok bit (sub block) dari *data stream* awal, yang masing-masing ditempatkan dalam *data stream* baru yang disebut sebagai *burst* seperti yang dilukiskan pada Gbr-1 di depan (*normal burst*). Kelompok bit tersebut berjumlah masing-masing 57 bit, sehingga terdapat 8 kelompok yang berasal dari 456

bit yang merupakan output blok *Channel coding*. Masing-masing kelompok bit tersebut ditempatkan dalam *burst* seperti ditunjukkan pada Gbr-7, sehingga terdapat 8 burst untuk setiap 456 bit. Setiap *burst* tersebut akan dikirimkan pada TDMA frame yang berbeda secara berurutan. Sehingga untuk 8 burst akan terkirim melalui 8 TDMA frame yang berurutan.

Tujuan proses interleaving ini adalah, menghindari resiko kehilangan deretan bit data yang ada dengan membuat duplikasinya untuk setiap 57 bit (*sub block*). *Sub block* dengan redundannya ditempatkan pada satu *burst* yang sama seperti ditunjukkan pada Gbr-7.

Proses de-interleaving terdiri dari proses sebaliknya dari proses interleaving. Waktu yang diperlukan untuk mengirimkan burst pertama ke burst ke delapan sama dengan 8 TDMA frame (sekitar 37 milisekon).

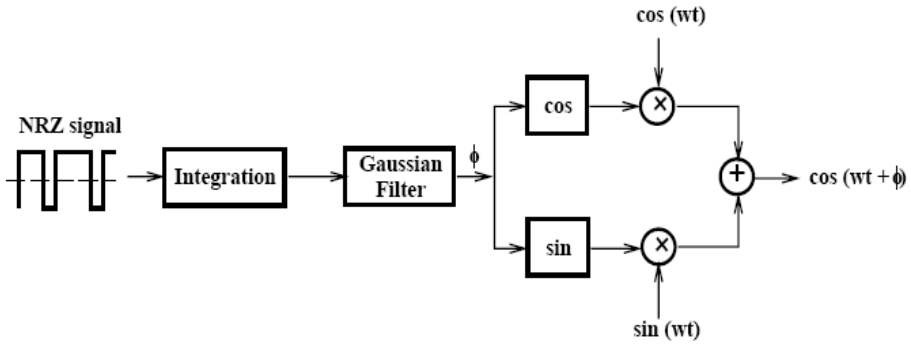
2.4 Proses *Chipering*

Ciphering adalah juga proses pengkodean dengan mengikuti algoritma tertentu, sehingga data lebih terlindungi lagi dari penyadapan. Data yang dimasudkan adalah, 2 x 57 bit yang ditempatkan dalam *normal-burst* tersebut. Proses dilakukan dengan mengacak ke 114 bit tersebut dan kemudian memroses melalui fungsi exclusive-OR. Urutan pengacakan didasarkan dari urutan *burst* dimana data itu berada dalam satu kombinasi bit yang disebut *key*. Data *key* telah dibuat sebelumnya dan dikirim melalui signaling oleh BTS.

Proses deciphering dilakukan mengikuti tahapan yang sebaliknya, termasuk data *key* yang merupakan satu set dengan data key waktu proses ciphering. Data *key* dapat sama ataupun berbeda untuk kedua proses tersebut.

2.5 Proses Modulasi

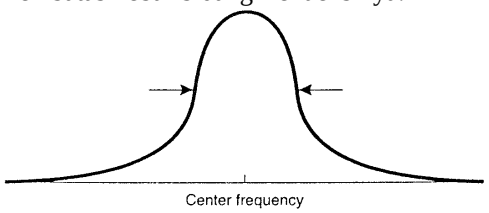
Diagram blok proses modulasi ditunjukkan pada Gbr-8, yaitu menggunakan teknik GMSK (*Gaussian filtered Minimum Shift Keying*), misalnya 0.39 GMSK, yang berarti bahwa 39% energi spektrum sinyal berada dalam batas nilai 3 dB nya, ***(1)p32***. Tanda '*x*' dan '+' masing-masing adalah fungsi perkalian dan penjumlahan. Dengan kedua proses itu, maka hasil akhirnya adalah fungsi *cos (ωt + φ)*. Disebut dengan nama Gaussian karena pada prosesnya menggunakan filter dengan tanggapan fungsi Gaussian seperti ditunjukkan pada Gbr-9. Fungsi utama filter ini adalah meningkatkan efisiensi spektrum energi yang diperlukan oleh sinyal digital.



Gambar 8 Diagram blok modulasi GMSK

Sinyal digital dengan format NRZ (*non return-to-zero*) adalah sinyal *burst* dengan *bit rate* 33,75 kbps hasil proses interleaving di depan. Jadi sinyal voice atau data itu telah mengalami proses coding dan ciphering seperti ditunjukkan pada Gbr-3. Sinyal NRZ ini kemudian mengalami proses integrasi, yaitu dengan rangkaian integrator, sehingga sinyal NRZ sebagai fungsi waktu bentuk persegi itu akan menjadi bentuk *ramp*.

Proses selanjutnya adalah pemilteran dengan menggunakan filter Gaussian untuk membatasi lebar bidang frekuensinya.



Gambar 9 Tanggapan frekuensi filter Gaussian

Output Gaussian filter kemudian di *split* menjadi dua untuk masing-masing dimodulasikan pada satu *carrier* tertentu yang berbeda fasa 90 derajat, yaitu, *cosinus* dan *sinus*. Hasil keduanya kemudian dicampur sehingga mendapatkan keluaran dengan bentuk $cos(\omega t + \varphi)$. Modulasi GMSK dipilih dalam sistem GSM ini karena pertimbangan efisiensi spektrum yang cukup tinggi mengingat sinyal informasi dengan format NRZ mempunyai spektrum yang relatif lebar.

3. Kesimpulan

Dari uraian pembahasan di Bagian-2, dapat disimpulkan bahwa sistem *mobile celluler phone* GSM merupakan sistem yang relatif aman dari penyadapan, diantaranya terdapat proses *ciphering* dalam pengolahan sinyalnya. Secara keseluruhan yang intinya sistem yang aman, dapat disimpulkan dalam butir-butir sebagai berikut:

a. Terdapat proses pengkodean-kanal (*channel-coding*) dengan algoritma tertentu, yaitu sinyal data digital dibentuk menjadi 260 bit untuk setiap 20 ms yang dibagi dalam tiga kelompok bit. Dua kelompok pertama yang perlu dilindungi, diproses lagi dengan proses convolution-code dengan satu polynomial tertentu seperti $G_1(x) = x^4 + x^3 + 1$. Dengan proses ini, jumlah 260 bit menjadi 456 bit. Jadi data sesungguhnya (*voice* atau data) sudah tidak nampak lagi, sehingga susah dikenali.

b. Terdapat proses *interleaving* dengan algoritma tertentu, yaitu, *bit stream* yang ber-jumlah 456 bit tersebut dibagi menjadi delapan *bit stream* yang masing-masing berisi 57 bit, jadi 8 x 57 bit. Masing-masing *bit stream* 57 bit ini kemudian disi-sipkan dalam *burst* (*normal-burst*) seperti ditunjukkan pada Gbr-7. Sehingga dengan proses *interleaving* ini, data makin disembunyikan.

c. Terdapat proses *ciphering* dengan algoritma tertentu, yaitu data yang berjumlah 2 x 57 = 114 bit diacak dengan ***key*** tertentu, sehingga tanpa mengetahui ***key*** untuk proses *deciphering*, maka penyadapan tidak dapat dilakukan.

d. Proses modulasi yang diterapkan pada sinyal GSM juga dapat dianggap khusus, karena sinyal yang berbentuk NRZ yang merupakan output blok-*ciphering* mengalami proses integration yang akhirnya dimodulasinya secara FSK. Proses modulasinya dikenal sebagai GMSK (*Gaussian Minimum Shift Keying*).

4. Daftar Pustaka

[1] Dayem, Rifaat A.; PCS & Digital Cellular Technologies-Assessing Your Options, Prentice Hall PTR, New Jersey, 1999.

[2] Turletti, Thierry; A brief Overview of the GSM Radio Interface, www.google.com, MIT, 1996.

[3] www.radio-electronics.com, What is GMSK Modulation, 2007

[4] www.sss-mag.com, Practical GMSK Data Transmission, 1995