INFORM : Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi
Vol.3 No.2, Juli 2018, P-ISSN : 2502-3470, E-ISSN : 2581-0367

Authentication Comparison of Telecommunications Technology Using A3, A8, A5 and Rijndael Algorithms

Ilham Arnomo
Universitas Hang Tuah
ilham.arnomo@hangtuah.ac.id

Abstract: The purpose of the research is to analyze the comparison of technology, network and security aspect between CDMA and GSM (Global System for Car communication). Using a comparative analysis research method between CDMA and GSM technologies that includes comparisons of network, technology, and security aspects. Using references from previous research on cellular telecommunications, the introduction of CDMA and GSM technologies to aspects of technology, networking and security. The results show that the technological aspect, CDMA used advanced spectrum technology that can provide superior sound quality and GSM uses a spectrum division technology that makes communication constant. From the network aspect, CDMA used direct-spreading spectrum (DS-CDMA) and GSM network is divided into three main systems: switching system (SS), base station system (BSS), and operating system and support (OSS). As well as security aspects, the GSM uses A3 and A8 algorithms for authentication and A5 algorithms were used in the process of sending information. But the security system using this algorithm, found weaknesses that allow data tapping or customer identity fraud. While CDMA offers aspects of network security by developing encryption algorithms. For encryption techniques used Rijndael algorithm is safe and very fast. A3 and A8 algorithms can recognize the customer's identity well, and the A5 algorithm can transmit the accuracy of information between MS and BTS.

Keyword: *Mobile Telecommunication; CDMA; GSM; A3 algorithm; A5 algorithm; A8 algorithm; Rijndael algorithm.*

Abstrak: Tujuan penelitian untuk menganalisis perbandingan teknologi, jaringan dan aspek keamanan antara telekomunikasi selular CDMA dan GSM *(Global System for Mobil communication)*. Menggunakan metode penelitian analisa komparatif antara teknologi CDMA dan GSM yang meliputi komparasi dari aspek jaringan, teknologi, dan keamanannya. Menggunakan referensi dari penelitian terdahulu tentang telekomunikasi selular, pengenalan teknologi CDMA dan GSM hingga aspek teknologi, jaringan dan keamanannya. Hasil penelitian menunjukkan bahwa aspek teknologi, CDMA menggunakan teknologi spektrum lanjutan yang dapat memberikan kelebihan kualitas suara yang tinggi dan GSM menggunakan sebuah teknologi pembagian spectrum yang membuat komunikasi dapat berjalan konstan. Dan dari aspek jaringan, CDMA menggunakan spectrum tersebar runtun langsung (DS-CDMA) dan jaringan GSM dibagi menjadi tiga sistem utama: sistem *switching* (SS), sistem *base station* (BSS), dan sistem operasi dan *support* (OSS). Serta dari aspek keamanan, pada GSM menggunakan algoritma A3 dan A8 untuk proses autentikasi serta algoritma A5 digunakan dalam proses pengiriman informasi, namun pada sistem pengamanan dengan menggunakan algoritma ini ditemukan kelemahan-kelemahan yang memungkinkan terjadinya penyadapan data ataupun penipuan identitas pelanggan. Sedangkan CDMA menawarkan aspek keamanan jaringan dengan mengembangkan algoritma enkripsi, untuk teknik enkripsi digunakan algoritma *Rijndael* yang aman dan sangat cepat. Algoritma A3 dan A8 dapat mengenali identitas pelanggan dengan baik, sedangkan algoritma A5 dapat mengirimkan akurasi informasi antara MS dengan BTS.

Kata kunci: Telekomunikasi Selular; CDMA; GSM; Algoritma A3; Algoritma A5; Algoritma A8; Algoritma Rijndael.

I. PENDAHULUAN

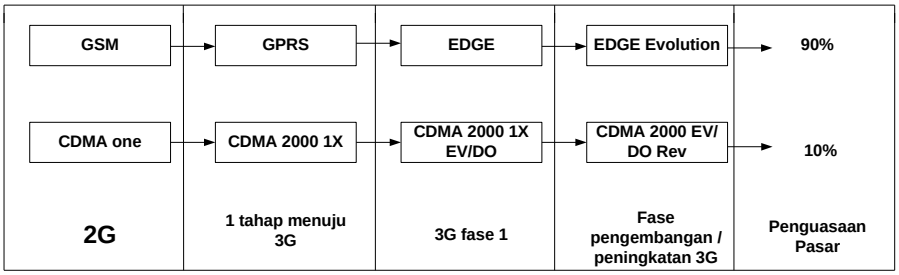
Semakin pesatnya kemajuan teknologi informasi dan komunikasi membutuhkan kemudahan dan kecepatan akses informasi dan komunikasi. Oleh karena itu sangat dibutuhkan suatu teknologi telekomunikasi yang dapat membantu kecepatan dan kemudahan dalam akses informasi dan komunikasi. Teknologi telekomunikasi tersebut adalah telekomunikasi bergerak atau yang biasa dikenal dengan telekomunikasi selular. Telekomunikasi selular ini dapat diaplikasikan dengan suatu perangkat komunikasi telepon selular. Adapun jenis teknologi telekomunikasi selular yang telah ada dan menjadi pilihan sesuai kebutuhan untuk media komunikasi, yaitu teknologi telekomunikasi selular CDMA (*Code Divison Multiple Access*) dan GSM . Sangat penting rasanya untuk cerdas memilih media komunikasi yang sangat tepat dengan mempertimbangkan beberapa aspek, misalnya aspek jangkauan jaringan telekomunikasinya; aspek kejernihan suara; hingga aspek pengiriman dan penerimaan data. Tentunya untuk keoptimalan penggunaan teknologi telekomunikasi

DOI : 10.25139/inform.v3i2.1031

selular juga tidak lepas dukungan dengan penggunaan perangkat telepon selular berspesifikasi tinggi dan dapat berfungsi *multitasking*, baik pada perangkat selularnya maupun fasilitas dan teknologi telekomunikasi selularnya.

Pada era teknologi informasi dan komunikasi sekarang, kebutuhan akan fungsi multitasking dan jangkuan jaringan telekomunikasi yang luas dan akses yang cepat, tentunya membutuhkan pembaruan fasilitas maupun teknologi telekomunikasi selular CDMA dan GSM untuk lebih variatif dan inovatif tanpa mengenyampingkan aspek keamanan dan kenyamanan berkomunikasi.

Telekomunikasi adalah teknik pengiriman atau penyampaian informasi dari suatu tempat ke tempat lain, sedangkan sebuah sistem telekomunikasi selular adalah komunikasi antar pesawat di mana salah satu pesawat bergerak atau berpindah lokasi dengan menggunakan sistem komunikasi tanpa kabel *(wireless)* [1] [2] [3] [4]. Teknologi telekomunikasi merupakan salah satu teknologi yang berkembang dengan sangat cepat, dimulai dengan layanan 1G sampai dengan 4G seperti yang ditunjukkan pada gambar 1. dan tabel 1 [3] [4] [5]. Perbandingan antara CDMA dengan GSM secara pada fase 2G ditunjukkan pada tabel 2 [4].



Gambar 1. Evolusi System Mobilisasi Telekomunikasi Menuju Teknologi 3G

Tabel 1. Perbandingan Teknologi Antar Generasi Telekomunikasi Bergerak

1G	2G	2,5G	3G
- Masih menggunaan teknologi Analog - Hanya layanan suara	- Beralih ke digital - Layanan utama masih voice - Layanan SMS - Untuk sambungan komputer dengan modem, kecepatan rendah (7-14Kbps)	- Teknologi antara (2G ke 3G) - Perubahan terhadap arsitektur 2G (min. GSM ke GPRS) - Layanan data yang lebih maju (min. WAP, ringtone, logo) - Arsitektur radio berubah untuk menghandle peningkatan bandwith - Human machine interface (min. PDA) - Color display - Bluetooth dan Wireless LAN	- Standar IMT-2000 - Kecepatan data 144 Kbps sampai 2 Mbps - Multimedia messaging - MPEG-4 Video - Akses internet kecepatan tinggi

Tabel 2. perbandingan antara CDMA dengan GSM secara pada fase 2G

Pembanding	**CDMA**	**GSM**
Keuntungan	Kecepatan akes data yang bisa didapat dengan teknologi ini adalah sekitar 153.6 kbps, suara yang lebih jernih, kapasitas yang lebih besar, dan kemampaun akses data yang lebih tinggi	Kemampuan *roaming* yang luas sehingga dapat dipakai diberbagai Negara
Kelemahan	Tingkat mobilitas terbatas	Kecepatan akses data pada jaringan GSM sangat kecil yaitu sekitar 9.6 kbps, karena pada awalnya hanya dirancang untuk penggunaan suara.
Teknologi	Digital	Digital
Tingkat moblitas	Terbatas dan dapat dikembangkan menjadi mobilitas penuh	Mobilitas penuh
	teknologi *Direct Sequence Spread Spectrum (DSSS)* dimana frekuensi radio 25 MHz pada band frekuensi 1800MHz dan dibagi dalam 42 kanal yang masing-masing kanal terdiri dari 30KHz	Teknologi akses gabungan antara FDMA*(Frequency Division Multiple Access)* dan TDMA *(Time Division Multiple Access)* yang awalnya bekerja pada frekuensi 900 Mhz

Pada generasi keempat teknologi telekomunikasi bergerak (3.5G dan 4G), untuk meningkatkan kecepatan akses data yang tinggi dan *full mobile* maka standar IMT-2000 di tingkatkan lagi menjadi 10Mbps,30Mbps dan 100Mbps yang semula hanya 2Mbps pada layanan 3G. Kecepatan akses tersebut didapat dengan mengguanakan teknologi OFDM *(Orthogonal Frequency Division Multiplexing)* dan *Multi Carrier*. 4G merupakan istilah yang umumnya digunakan mengacu kepada pengembangan teknologi telepon selular. 4G merupakan pengembangan dari teknologi 3G. Nama resmi dari teknologi 4G ini menurut IEEE *(Institute of Electrical and Electronics Engineers)* adalah *"3G and beyond"*. Sistem 4G dapat menyediakan solusi IP yang komprehensif dimana suara, data, dan arus multimedia dapat sampai kepada pengguna kapan saja dan dimana saja, pada rata-rata data lebih tinggi dari generasi sebelumnya. Bagaimanapun, terdapat beberapa pendapat yang ditujukan untuk 4G, yakni: 4G merupakan sistem berbasis IP terintegrasi penuh. Ini akan dicapai setelah teknologi kabel dan nirkabel dapat dikonversikan dan mampu menghasilkan kecepatan 100Mb/detik dan 1Gb/detik baik dalam maupun luar ruang dengan kualitas premium dan keamanan tinggi [4][2][3].

DOI : 10.25139/inform.v3i2.1031

Teknologi 4G (*Fourth Generation*) adalah teknologi kelanjutan dari proses perkembangan teknologi telepon selular (*mobile phone*). Sebelumnya ada teknologi 2G (*Second Generation*) yang sangat ngetrend dengan teknologi voice call dan SMS. Selanjutnya teknologi 3G (*Third Generation*) dengan andalannya teknologi *video call*. Di generasi keempat (4G), akan cenderung dibawa pada sebuah koneksi yang bisa selalu terhubung setiap saat. Atau bisa dijabarkan dengan istilah kapan saja, dimana saja dan bahkan dengan perangkat apa saja. Istilah 4G digunakan secara luas untuk menggabungkan beberapa macam sistem komunikasi *broadband wireless access* ke dalam sebuah sistem komunikasi dan bukan hanya sistem telepon selular saja melainkan juga menunjang keberadaan *fixed wireless network* seperti Wi Fi (*Wireless Fidelity*) dan Wi Max (*Wireless Metropolitan Access*). Oleh karena itu, sistem 4G diharapkan menjadi sebuah sistem yang mampu menjembatani antara berbagai jaringan *broadband wireless access* yang telah ada secara *seamlessly* (tidak terasa proses perpindahan antar jaringan yang sedang digunakan) baik perangkatnya, maupun jaringannya dan juga aplikasinya [4].

Penelitian tentang perbandingan teknologi bergerak CDMA dengan GSM pernah dilakukan oleh [6], hasil penelitiannya menunjukkan bahwa yang awalnya teknologi handset CDMA yang berbasis chip kurang diminati dan banyak keterbatasan saat digunakan untuk berkomunikasi secara mobile serta masih tertinggal dengan teknologi handset GSM yang menggunakan kartu SIM *(Subscriber Identity Module)*[6]. Akhirnya CDMA meluncurkan teknologi *Removable User Identity Module* (RUIM).

Berdasarkan hasil analisis gap, perlu dikembangkan penelitian tentang analisis perbandingan teknologi telekomunikasi selular CDMA dan GSM, dengan tujuan penelitian membandingkan aspek teknologi, jaringan dan keamanan menggunakan algoritma A3, A8, A5 dan Rijndael.

II. METODE PENELITIAN

Menggunakan metode penelitian analisa komparatif antara teknologi telekomunikasi selular CDMA dengan GSM yang meliputi perbandingan jaringan, teknologi, dan aspek keamanannya. Sumber data dan informasi yang digunakan adalah data dan informasi dari referensi penelitian terdahulu tentang telekomunikasi selular, pengenalan teknologi CDMA dan GSM hingga aspek teknologi, jaringan dan keamanannya.

III. HASIL DAN PEMBAHASAN

CDMA merupakan singkatan dari teknik akses jamak (*Multiple Access*) yang berarti dapat memisahkan percakapan dalam domain kode [7] [8]. CDMA merupakan teknologi digital tanpa kabel (*Digital Wireless Technology*) yang pertama kali dibuat oleh perusahaan Amerika–*Qualcomm*. CDMA**,** menggunakan teknologi *spread-spectrum* untuk mengedarkan sinyal informasi yang melalui *bandwith* yang lebar yaitu 1,25 MHz. Teknologi ini asalnya dibuat untuk kepentingan militer, menggunakan kode digital yang unik, lebih baik daripada channel atau frekuensi RF (*radio frekuensi*). Sistem CDMA dinilai lebih *advance* dibanding sistem selular digital yang sudah mempunyai FSN (*frekuensi serial number*) mampu memberikan suara alami yang lebih sempurna dibandingkan dengan sistem selular digital GSM. Serta power output yang sangat rendah yakni 0,2 watt dibanding dengan system GSM yang menggunakan power output sebesar 1,5 - 3 watt, sehingga dapat menjadikan baterei pada ponsel yang menggunakan teknologi atau sistem CDMA lebih tahan lama untuk melakukan percakapan atau dalam berkomunikasi [4].

A.1 Fitur teknologi CDMA [4]*:*

Teknologi CDMA didesain tidak peka terhadap interferensi (masuknya suatu gangguan suara dari lingkungan luar jalur telekomunikasi yang menyebabkan hilangnya sebagian informasi). Sejumlah pelanggan dalam satu sel dapat mengakses pita spektrum frekuensi secara bersamaan karena mempergunakan teknik pengkodean yang tidak bisa dilakukan pada teknologi GSM, hal ini berarti teknologi CDMA sangat efisien dalam penggunaan frekuensi, karena tidak memerlukan frekuensi baru dalam menyediakan layanan komunikasi yang interaktif sehingga tidak menambah biaya pengadaan frekuensi baru. Kapasitas yang lebih tinggi untuk mengatasi lebih banyak panggilan yang simultan per *channel* dibanding sistem yang ada. Sistem CDMA menawarkan peningkatan kapasitas melebihi system AMPS (*Advanced Mobile Phone Service)* analog sebaik teknologi selular digital lainnya. CDMA menghasilkan sebuah skema *spread spectrum* yang secara acak menyediakan bandwith 1.250 KHz yang tersedia untuk masing-masing pemanggil 9600 bps bit rate. Meningkatkan *call security*. Keamanan menjadi sifat dari pendekatan *spread spectrum* CDMA, dan kenyataannya teknologi ini pertama dibangun untuk menyediakan komunikasi yang aman bagi militer, dan juga dapat mereduksi derau dan interferensi lainnya.

CDMA menaikkan rasio *signal-to-noise* (CDMA dapat menaikkan selisih sinyal dari noise atau gangguan), karena lebarnya *bandwith* yang tersedia untuk pesan. Efisiensi daya dengan cara memperpanjang daya hidup baterai ponsel berteknologi CDMA. Salah satu karakteristik CDMA adalah kekuatan kendali sebuah usaha untuk memperbesar kapasitas panggilan dengan memepertahankan kekonstanan level daya yang diterima dari pemanggil bergerak pada *base station*. Fasilitas kordinasi seluruh frekuensi melalui *base-station base station*. Sistem CDMA menyediakan *soft hand-off* dari satu *base-station* ke *base-station* lainnya sebagai sebuah roaming telepon bergrak dari sel ke sel, melakukan *soft handoff* dikarenakan semua sistem menggunakan frekuensi yang sama [1]. Fungsi *spread-spectrum* dan kekuatan kendali yang memperbesar kapasitas panggil CDMA mengakibatkan *bandwith* yang cukup untuk bermacam-macam layanan data multimedia, dan skema *soft hand-off* menjamin: Tidak hilangnya data, meningkatkan kualitas suara, memperbaiki karakteristik cakupan yang dapat menurunkan jumlah sel, meningkatkan *privacy* dan *security*, menyederhanakan perencanaan sistem, memerlukan daya pancar yang lebih rendah, sehingga waktu bicara ponsel dapat lebih lama,

DOI : 10.25139/inform.v3i2.1031

mengurangi interferensi pada sistem lain, lebih tahan terhadap multipath, dapat dioperasikan bersamaan dengan teknologi lain (misal AMPS (*Advanced Mobile Phone Service)*).

A.2 Broadband CDMA

Teknologi Broadband CDMA merupakan teknologi spektrum lanjutan yang digunakan untuk kepentingan komersil dan dapat memberikan berbagai kelebihan dibanding dengan system komunikasi lainnya. Kelebihan-kelebihan tersebut meliputi kualitas suara yang tinggi, karakteristik *fade* dan performansi *indoor* (dalam ruangan) yang sangat baik serta dinamika rata-rata data yang baik. Perbedaan yang ditekankan antara *narrow* CDMA dengan *Broadband* CDMA adalah kelebihan *broadband* yang didesain untuk menggunakan *bandwidth* yang beraneka ragam mulai dari 7 MHz sampai 15 MHz. Dengan *bandwidth* yang besar maka akan tersedia juga *level of fade resistance* (resistensi terhadap menghilangnya sinyal) yang lebih besar menghasilkan *performance* atau kinerja yang lebih baik untuk power dan menghemat power untuk menyediakan *power coverage* tertentu. *Bandwidth* yang lebih besar juga menyebabkan kapasitas yang juga bertambah untuk mendukung berbagai macam layanan yang lebih tinggi dan meningkatkan feksibilitas untuk gabungan layanan. Ini berarti sebuah sistem *broadband* bisa melayani beraneka ragam layanan secara keseluruhan[4]. Keuntungan *Broadband* CDMA adalah fleksibitas tinggi yang ditawarkan. Sistem CDMA sendiri menawarkan penghitungan biaya yang efektif baik dalam skala komunikasi besar ataupun skala kecil. Dengan Broadband CDMA, kita dapat mengakses layanan suara dan data seperti facsimile, email, dan kecepatan internet yang tinggi [4]. Selain itu *broadband* CDMA dapat ditambah ke jaringan yang sedang aktif tanpa adanya penundaan dan gangguan dari kabel telepon. Hubungan ke jaringan LAN (*Local Area Network*) untuk pengiriman email dan pembagian sumber jaringan seperti mesin printer dan faksimile dapat dilakukan dengan mudah. Sistem *broadband* juga dapat mengurangi efek penggandaan sistem pada kondisi yang sebenarnya dan menyebarkan frekuensi dari 7MHz sampi dengan 30 MHz. *Broadband* CDMA memiliki beberapa aplikasi utama yang ditawarkan yaitu *Rural Wireless Local Loop* (Rural WLL), *Urban Wireless Local Loop* (Urban WLL), *Personal Communication System* (PCS), dan *Global Mobile Personal Communications by Satellite* (GMPCS) [4].

A.3 Sistem Komunikasi CDMA

Sistem komunikasi CDMA adalah suatu sistem komunikasi yang berakses jamak yang menerapkan pembagian teknik akses komunikasi berdasarkan pembagian frekuensi, pembagian waktu dan pembagian sandi [4] [8] [9]. Masalah utama dalam komunikasi radio CDMA adalah terbatasnya alokasi frekuensi, sehingga penggunaannya harus benar-benar terkendali. Tiga teknik akses jamak yang sering digunakan yaitu teknik akses jamak pembagian frekuensi (*Frekuensi Division Multiple Access atau* FDMA), teknik akses jamak pembagian waktu TDMA (*Time Division Multiple Access*), dan teknik akses jamak pembagian sandi *CDMA*. Dalam hal ini hanya akan dibahas akses jamak pembagian sandi CDMA [4]. Kondisi ini akan menurunkan unjuk-kerja sistem. Ini berarti, kapasitas dan kualitas sistem dibatasi oleh daya interferens yang timbul pada lebar bidang frekuensi yang digunakan [4] [8] [9].

A.4 Sistem Spektrum Tersebar

Sistem transmisi spektrum tersebar adalah sebuah teknik yang mentransmisikan suatu isyarat dengan lebar bidang frekuensi tertentu menjadi suatu isyarat yang memiliki lebar bidang frekuensi yang jauh lebih besar. Aliran data asli dikalikan secara biner dengan sandi penyebar yang memilki lebar bidang yang jauh lebih besar daripada isyarat asal. Bit-bit dalam sandi penyebar dikenal dengan *chip* untuk membedakannya dengan bit-bit dalam aliran data yang dikenal dengan simbol[4][9]. Setiap pengguna memiliki sandi penyebar yang berbeda dengan pengguna yang lain. Sandi yang sama digunakan pada kedua sisi kanal radio, menyebarkan isyarat asal menjadi isyarat bidang lebar, dan menyebarkan kembali isyarat bidang lebar menjadi isyarat bidang sempit asal. Penyebaran antara lebar bidang transmisi dengan lebar bidang isyarat asal dikenal dengan *processing gain.* Secara sederhana, *processing gain* menunjukkan berapa buah *chip* yang digunakan untuk menyebarkan sebuah simbol data. Sandi-sandi penyebar bersifat unik, jika seorang pengguna telah mengawasebarkan isyarat bidang lebar yang diterima, isyarat yang dibawasebarkan hanyalah isyarat dari pengirim yang memiliki sandi penyebar yang sama [4][9].

Sebuah sandi penyebar memilki korelasi-silang yang rendah dengan sandi penyebar yang lain. Jika sebuah sandi benar-benar ortogonal, maka korelasi-silang antara sebuah sandi dengan sandi yang lainnya adalah nol. Hal ini berarti beberapa isyarat bidang lebar dapat menggunakan frekuensi yang sama tanpa adanya interferens satu sama lain. Energi isyarat bidang lebar disebarkan sepanjang lebar bidang yang amat besar sehingga dapat dianggap sebagai derau jika dibandingkan dengan isyat aslinya atau dengan kata lain memiliki *power spectral density* yang rendah. Ketika sebuah isyarat bidang lebar dikorelasikan dengan sandi penyebar tertentu, hanya isyarat dengan sandi penyebar yang sama yang akan diawasebarkan, sedangkan isyarat dari pengguna lain akan tetap tersebar [4] [9].

Sistem spektrum tersebar memiliki beberapa kelebihan dapat bertahan pada lingkungan dengan pudaran lintasan jamak yang tinggi karena isyarat CDMA bidang lebar memiliki sandi penyebar dengan sifat korelasi-diri yang baik, mengirimkan informasi dengan daya yang kecil sehingga memungkinkan peralatan yang kecil sekaligus juga dengan daya baterai yang lebih tahan lama, mengurangi interferen dengan baik karena pada saat terjadinya proses pengawasebaran pengganggu akan mengalami proses sebaliknya sehingga dayanya akan lebih kecil dibandingkan isyarat asli, menghindari penyadapan karena menggunakan sandi unik yang mirip derau dengan spektrum frekuensi yang amat lebar, melakukan kemampuan panggilan terpilih (*selective calling capability*) dan melakukan penjamakan pembagian sandi sehingga dimungkinkan untuk akses jamak dengan kapasitas yang lebih besar.

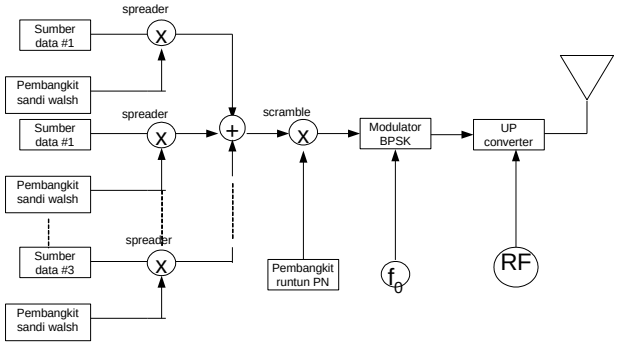
DOI : 10.25139/inform.v3i2.1031

A.5 Model Pengirim dan Penerima Sistem CDMA

Sistem CDMA dapat dimodelkan secara sederhana menggunakan spectrum tersebar runtun langsung (DS-CDMA) seperti pada gambar 2. Pemodelan di sini dibatasi untuk kanal maju (*forward channel*) atau *downlink,* yaitu transmisi dari BTS ke MS. Model ini dibedakan menjadi bagian Pengirim dan Penerima. Data digital dari satu pengguna dikalikan secara *modulo-2* dengan sandi penyebar (*spreader*) Walsh, yang merepresentasikan 1 kanal komunikasi. Hasil proses *spreading* tersebut kemudian dijumlahkan (dijamak) dengan kanal-kanal lain yang mempunyai sandi Walsh berbeda, Isyarat hasil penjamakan tersebut diacak (*scrambling*) oleh sebuah runtun PN (*Pseudo-Random Noise*) dengan panjang tertentu. Setelah itu, isyarat dimodulasi secara BPSK (*Biphase Shift Keying*) dengan pembawa berfrekuensi *fo.* Sebelum ditransmisikan isyarat dinaikan frekuensinya oleh bagian *Up-Converter* untuk mencapai frekuensi radio (*Radio Frekuensi*, RF).

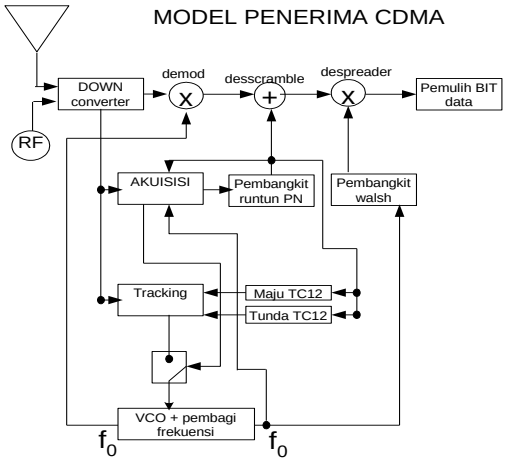
A.6 Model Jaringan CDMA

Jaringan CDMA menawarkan aspek keamanan jaringan dengan mengembangkan algoritma enkripsi. Untuk teknik enkripsi digunakan algoritma Rijndael yang aman dan sangat cepat, pada autentifikasi menggunakan prosedur *Unique Challenge Procedure* dimana *base station* membangkitkan nilai 24-bit *value* dan mentransmisikannya ke *mobile station* di *Authentication Challenge Message.* Teknologi CDMA membuat kesulitan terhadap kegiatan penyadapan, baik yang bersifat terus menerus maupun sesaat karena mengimplementasikan 42-bit PN (*Pseudo-Random Noise*) sekuens yang disebut dengan "*Long Code"* [4].



Gambar 2. Model Pengirim CDMA

Sedangkan pemrosesan isyarat pada penerima [4] dilakukan dengan isyarat diterima diturunkan frekuensinya hingga mencapai frekuensi *fo* oleh *Down-Converter*. Data dipulihkan, runtun PN (*Pseudo-Random Noise*), sandi Walsh dan detak penerima haruslah sinkron dengan pengirim. Proses sinkronisasi melibatkan runtun PN dengan dua tahapan, yaitu sinkronisasi kasar (akuisisi) dan sinkronisasi halus (*tracking*). Setelah runtun PN, sandi Walsh dan detak penerima sinkron dengan pengirim, maka dilakukan proses demodulasi oleh *demodulator*. Demodulasi mengalikan detak yang mempunyai frekuensi sebesar *fo* dengan isyarat keluaran *down converter.* Proses selanjutnya adalah *descrambling,* yaitu mengalikan dengan runtun PN (*Pseudo-Random Noise*) penerima. Hasil proses *descrambling* dikalikan dengan Walsh penerima yang disebut proses pengawasebaran (*despreading*), data akan terpulihkan jika sandi Walsh penerima identik dengan salah satu sandi Walsh pengirim.



Gambar 3. Model Penerima CDMA

A.7 Aspek Keamanan Yang Disediakan CDMA

Autentifikasi, merupakan proses dimana informasi dipertukarkan antara *mobile station* dan *base station* untuk mengkonfirmasikan identitas mobile station. Prosedur autentifikasi signature (*Auth_Signature*) digunakan untuk menampilkan autentifikasi untuk *mobile station* tertentu [4] [10]. Parameter input berikut ini merupakan syarat dalam prosedur ini yakni RAND_CHALLENGE, ESN, AUTH_DATA, SSD_AUTH dan SAVE_REGISTERS [4] [10]. Autentifikasi ditampilkan menggunakan prosedur *Unique Challenge Procedure*[10].

Base station membangkitkan nilai 24-bit value dan mentransmisikannya ke *mobile station* di *Authentication Challenge Message*. Tergantung pada catatan pesan, *mobile station* melaksanakan prosedur *Auth_Signature* dan field AUTHU dibangkitkan, yang mana telah dikirim ke *base station* melalui *Authentication Challenge Response Message*. *Base station* juga melaksanakan prosedur *Auth_Signature* menggunakan nilai yang disimpan secara internal, dan *output* dibandingkan dengan nilai AUTHU pada PDU yang diterima. Jika autentifikasi gagal, maka akses selanjutnya melalui *mobile station* ditolak dan prosedur *updating* SSD dapat dilakukan [4]. Desain teknologi CDMA membuat kesulitan terhadap kegiatan penyadapan, baik yang bersifat terus menerus maupun sesaat. Hal yang unik dari sistem CDMA adalah 42-bit PN (*Pseudo-Random Noise*) sekuens yang disebut dengan "*Long Code*" ke perebutan suara dan data. Pada *forward* link (jaringan ke *mobile*), data diperebutkan pada *rate* 19.2 Kilo simbol per detik (Ksps) dan pada *reverse link* , data diperebutkan pada *rate* 1.2288 Mega chips per detik (Mcps) [4]. Protokol jaringan keamanan CDMA berada pada 64-bit *authentication key* (A-Key) dan *Electronic Serial Number* (ESN) dari *mobile*. Angka acak yang disebut *RANDSSD* yang dibangkitkan pada HLRatauAC, juga menjalankan peran dalam prosedur *authentication*. *A-Key* diprogram dalam mobile dan disimpan

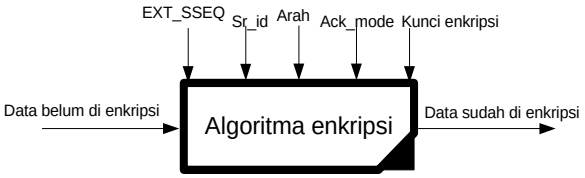
DOI : 10.25139/inform.v3i2.1031

dalam *Authentication Center (AC*) jaringan. Sebagai tambahan pada *authentication*, yakni bahwa *A-Key* digunakan untuk membangkitkan sub-key untuk *privacy* suara dan *message encryption* [4]. CDMA menggunakan standarisasi algoritma CAVE (*Cellular Authentication dan Voice Encryption)* untuk membangkitkan 128-bit *subkey* yang disebut "*Shared Secret Data*" (SSD). A*Key*, *ESN* dan jaringan-supplied *RANDSSD* merupakan input ke CAVE yang membangkitkan SSD. SSD memiliki dua bagian: SSD_A (64 bit), untuk membuat *authentication signatures* dan SSD_B (64 bit), untuk membangkitkan kunci untuk *encrypt* pesan suara dan signal. SSD dapat di *share* dengan memberikan layanan untuk memungkinkan *local authentication*. SSD yang baru dapat digenerate ketika *mobile* kembali ke jaringan *home* atau *roam* ke sistem yang berbeda [4]. Jaringan CDMA, *mobile* menggunakan SSD_A dan broadcast RAND* sebagai input terhadap algoritma CAVE untuk membangkitkan 18-bit *authentication signature* (*AUTH_SIGNATURE),* dan mengirimkan ke *base station*. *Signature* ini juga kemudian digunakan oleh *base station* untuk memverifikasi legitimasi *subscriber*. Metode *Global Challenge* memungkinkan terjadi *autentication* dengan sangat cepat. Juga, baik *mobile* dan *track* jaringan *Call History Count* (6-bit counter). Hal ini memberikan jalan untuk mendeteksi terjadinya pengkloningan, sebagaimana operator mendapat sinyal jika ada gangguan [4].

A-Key dapat diprogram ulang, tapi *mobile* dan jaringan *Authentication Center*harus diupdate. A-key kemungkinan dapat diprogram oleh salah satu dari vendor berikut: Pabrik; Dealer pada point penjualan; Subscriber via telepon; dan OTASP (over the air service provisioning) [4] [10]. Transaksi OTASP memanfaatkan 512-bit perjanjian algirtma Diffie - Hellman key, membuat aman secara fungsi. A-Key pada mobile dapat diubah melalui OTASP, memberikan cara yang mudah agar cepat memotong layanan (*cut off service*) untuk di kloning secara *mobile* atau membuat layanan baru untuk melegitimasi subscriber. Keamanan A-Key merupakan komponen terpenting dalam sistem CDMA [4] [10].

Proteksi (Voice, Signal, Data Privacy). *Mobile* menggunakan SSD_B dan algoritma CAVE untuk membangkitkan *Private Long Code Mask* (diturunkan dari nilai intermediate yang disebut *Voice Privacy Mask,* yang mana menggunakan sistem legacy TDMA (*Time Division Multiple Access*)), *Cellular Message Encryption Algorithm* (CMEA) key (64 bits), dan Data Key (32 bits). *Private Long Code Mask* memanfaatkan *mobile* dan jaringan untuk mengubah karakteristik *Long code*. *Private Long Code Mask* tidak mengenkripsi informasi, hal ini mudah memindahkan nilai yang telah dikenal dengan baik dalam mengencode sinyal CDMA dengan nilai private yang telah dikenal baik untuk mobile maupun jaringan. Hal ini sangat ekstrim sulit untuk menyadap percakapan tanpa tahu *Private Long Code Mask*. Sebagai tambahan, *mobile* dan jaringan menggunakan key CMEA dengan algoritma Enhanced CMEA (ECMEA) untuk mengenkripsi pesan sinyal dikirim melalui udara dan di dekripsi informasi yang diterima. Kunci data terpisah, dan algoritma enkripsi disebut ORYX, digunakan oleh mobile dan jaringan untuk mengenkripsi dan mendekripsi lalu lintas data pada saluran CDMA [4]. Desain semua telepon CDMA menggunakan kode PN (Pseudo-random Noise) yang unik untuk memperluas sinyal, yang mana hal ini membuat sinyal menjadi sulit untuk disadap [4].

Anonimity, merupakan teknik enkripsi pada gambar 4 yang digunakan dalam sistem 1xEV-DV sama dengan yang digunakan pada CDMA2000.



Gambar 4. Enkripsi dalam CDMA 1xEV-DV

Mobile station mengindikasikan ke *base station*, beberapa variasi algoritma enkripsi yang mendukungnya. *Base station* mempunyai keleluasaan untuk memutar *onatauoff* enkripsi sinyal data atau informasi data pengguna. *Mobile station* juga dapat mengusulkan untuk memutar enkripsi menjadi *onatauoff*. Pesan-pesan tidak dienkripsi jika autentifikasi tidak ditampilkan untuk pesan khusus. Selain itu juga, pesan-pesan yang pendek dikirimkan tanpa dienkripsi. Pesanpesan yang membawa kapasitas *field* enkripsi cukup bervariasi berdasarkan nilai P_REV dari *mobile station*. Algoritma enkripsi yang digunakan 1xEV-DV adalah *Rijndael Encryption Algorithm* [4]. Algoritma enkripsi Rijndael merupakan algoritma yang aman dan sangat cepat. Algoritma enkripsi Rijndael memungkinkan hanya ukuran kunci 128, 192 dan 256-bit [10]. Kunci yang digunakan sudah dikembangkan untuk pengaturan *n* round keys. Oleh sebab itu, input data berjalan dengan operasi *rounds*. Algorithm yang digunakan untuk enkripsi dispesifikasikan melalui field SDU_ENCRYPT_MODE variasi pesan layer 3. Jika enkripsi ditampilkan dalam yang ditransmisikan pada layer 3, maka menggunakan SDU, sebagaimana panjangnya menjadi terintegral multiple 8. 8-bit CRC dihitung pada data dan bit-bit CRC dilampirkan pada data [4] [10].

Tabel 3. Field Enkripsi

Field	Keterangan
EXT_SSEQ	32-bit urutan jumlah enkripsi keamanan untuk enkripsi / dekripsi
Sr_id	*Identifier*, layanan referensi untuk pilihan layanan cepat yang terkait
Arah	Arah data yang dienkripsi/dekripsi/ hal itu di set dengan "0" jika data diterima/dikirim pada kanal pengiriman, selain itu di set "1"
Kunci enkripsi	Kunci session untuk enkripsi. Hal ini merupakan hasil sukses perjanjian kunci. Session antara mobile station dan base station

DOI : 10.25139/inform.v3i2.1031

Field	Keterangan
Ack_mode	Mode pengiriman pesan. Hal ini diatur dengan set "0" jika pesan terkirim menggunakan mode un-assured dan yang lainnya di set "1"

A.8 Keunggulan Teknologi CDMA [4]:

Teknologi CDMA didesain tidak peka terhadap interferensi. Di samping itu, sejumlah pelanggan dalam satu sel dapat mengakses pita spektrum frekuensi secara bersamaan karena mempergunakan teknik pengkodean yang tidak bisa dilakukan pada teknologi GSM. Kapasitas yang lebih tinggi untuk mengatasi lebih banyak panggilan yang simultan per channel dibanding system yang ada. Sistem CDMA menawarkan peningkatan kapasitas melebihi system AMPS (*Advanced Mobile Phone Service)* analog sebaik teknologi selular digital l ainnya. CDMA menghasilkan sebuah skema *spread spectrum* yang secara acak menyediakan bandwith 1.250 KHz yang tersedia untuk masingmasing pemanggil 9600 bps bit rate.

Dari segi keamanan panggilan, keamanan menjadi sifat dari pendekatan spread spectrum CDMA, dan kenyataannya teknologi ini pertama dibangun untuk menyediakan komunikasi yang aman bagi militer. Mereduksi derau dan interferensi lainnya. CDMA menaikkan rasio *signal-to-noise*, karena lebarnya *bandwith* yang tersedia untuk pesan. Efisinsi daya dengan cara memperpanjang daya hidup baterai telepon.

Salah satu karakteristik CDMA adalah kekuatan kendali sebuah usaha untuk memperbesar kapasitas panggilan dengan mempertahankan kekonstanan level daya yang diterima dari pemanggil bergerak pada base station. Fasilitas kordinasi seluruh frekuensi melalui base-station base station. Sistem CDMA menyediakan soft hand-off dari satu base-station ke lainnya sebagai sebuah roaming telepon bergerak dari sel ke sel, melakukan *soft handoff* mengingat semua sistem menggunakan frekuensi yang sama. Fungsi *spread-spectrum* dan kekuatan kendali yang memperbesar kapasitas panggil CDMA mengakibatkan *bandwith* yang cukup untuk bermacam-macam layanan data multimedia, dan skema *soft hand-off* menjamin : Tidak hilangnya data; Meningkatkan kualitas suara; Memperbaiki karakteristik cakupan yang dapat menurunkan jumlah sel; Meningkatkan *privacy* dan *security*; Menyederhanakan perencanaan system; Memerlukan daya pancar yang lebih rendah, sehingga waktu bicara ponsel dapat lebih lama; Mengurangi interferensi pada sistem lain; Lebih tahan terhadap multipath dan Dapat dioperasikan bersamaan dengan teknologi lain (misal AMPS (*Advanced Mobile Phone Service)*).

IV. PENGENALAN GSM

GSM merupakan standar yang diterima secara global untuk komunikasi selular digital. GSM menggunakan teknologi akses TDMA *(Time Division Multiple Access)*, yang mana merupakan sebuah teknologi digital sama halnya yaitu dengan membagi-bagi spektrum yang tersedia kepada sejumlah channel diskrit yang tetap, meskipun masing-masing channel merepresentasikan time slot yang tetap daripada band frekunesi yang tetap [4]. GSM adalah nama group standardisasi yang di mapankan pada tahun 1982 untuk menghasilkan standar telepon bergerak di eropa, digunakan sebagai formula spesifikasi untuk pan-eropa system selular radio bergerak yang bekerja pada frekuensi 900 Mhz. Dan diperkirakan banyak negara lainnya diluar eropa akan turut menggunakan teknologi GSM [4] [11]. Jaringan GSM bertujuan untuk memperbaiki masalah tersebut dengan mengimplementasikan autentifikasi yang kuat antara telepon selular dan MSC (*mobile service switch center*), mengimplementasikan enkripsi data yang kuat pada transmisi udara antara MS dan BTS [4].

Keamanan dan mekanisme autentifikasi yang terdapat pada GSM membuat GSM sebagai jaringan komunikasi yang aman, khususnya jika dibandingkan dengan sistem analog. Bagian yang menjadikan GSM aman yaitu adanya sistem digital yang mengenkripsikan pembicaraan, GMSK (*Gaussian Minimum Shift Keying*) modulasi digital, dan TDMA (*Time Division Multiple Access*). Untuk memotong dan merekonstruksi sinyal GSM diperlukan peralatan yang khusus dan mahal [4]. Spesifikasi GSM tidak disebarluaskan ke umum untuk mencegah terjadinya pembelajaran tentang proses autentifikasi dan algoritma enkripsi terhadap model keamanan GSM. Konsorsium GSM berdasar atas prinsip keamanan dengan ketidakkenalan, maksudnya adalah algoritma enkripsi akan sulit di pecahkan jika algoritma tersebut tidak dipublikasi [4]. Menurut suatu komunitas sains, salah satu syarat untuk menjaga keamanan suatu algoritma adalah keamanan pada sistem kriptografinya, ini berarti keamanan hanya terdapat pada kuncinya. Pendapat ini terkenal dengan asumsi Kerckhoffs' [4]. Algoritma seharusnya harus dipublikasi, sehingga algoritma itu dapat diteliti oleh masyarakat umum. Dengan itu dapat diketahui seberapa kuat algoritma tersebut. Kondisi berbeda terjadi jika algoritma tidak dipublikasi, suatu ketika mungkin algoritma tersebut mengalami kesalahan desain sehingga sebenarnya sangat mudah dipecahkan. Jaringan GSM saat ini digunakan algoritma A3, A8, dan A5 dalam sistem pengamanannya. Algoritma A3 dan A8 digunakan dalam proses autentikasi, yaitu proses pengenalan identitas pelanggan, yang terjadi pada MS (*Mobile Station*) dan AUC (*Authentication Centre*) Sedangkan algoritma A5 digunakan dalam proses pengiriman informasi pada link radio antara MS dengan BTS (*Base Transceiver Station*). Namun pada sistem pengamanan dengan menggunakan algoritma ini ditemukan kelemahan-kelemahan yang memungkinkan terjadinya penyadapan data ataupun penipuan identitas pelanggan [4].

B.1 Jaringan GSM

Jaringan GSM dibagi menjadi tiga sistem utama: sistem *switching* (SS), sistem *base station* (BSS), dan sistem operasi dan support (OSS) [4] [12]. Elemen dasar jaringan GSM di tunjukkan pada gambar 5 [4].

a. Sistem *switching* bertanggung jawab untuk melakukan proses panggilan dan fungsi pelanggan. Sistem switching mencakupi fungsional unit [4]. *Home Location Register* (HLR), merupakan suatu basis data yang digunakan untuk menyimpan dan mengatur abonemen. HLR mempertimbangkan basis data yang paling penting, dimana

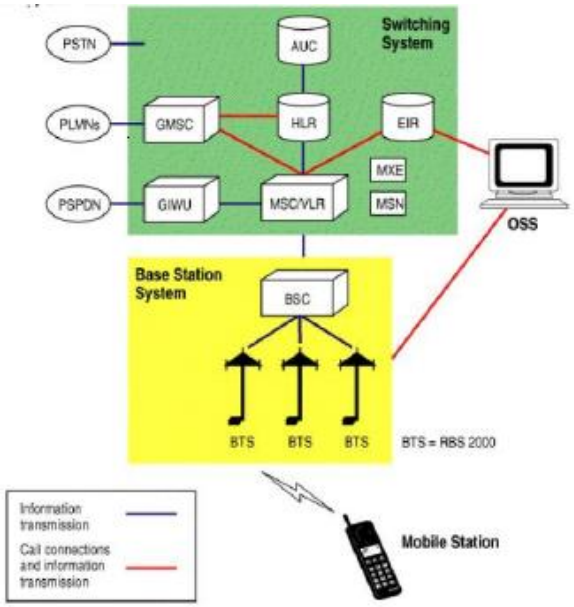
DOI : 10.25139/inform.v3i2.1031

menyimpan data secara permanen tentang pelanggan, termasuk layanan profile nya, informasi lokasi, dan status aktivitas. Ketika perseorangan menjadi pelanggan dari suatu operator PCS, maka dia telah terdaftar di HLR operator tersebut. *Mobile Services Switching Center* (MSC), melakukan fungsi telepon switching dari suatu sistem. MSC mengontrol panggilan ke dan dari telepon lainnya dan sistem data. Dan juga melakukan fungsi sebagai toll ticketing, antarmuka jaringan, pensinyalan kanal umum, dan lainnya. *Visitor Location Register* (VLR), basis data yang berisi informasi sementara tentang pelanggan, dimana diperlukan oleh MSC untuk melayani pelanggan yang datang berkunjung. VLR selalu terintegrasi dengan MSC. Ketika stasion bergerak menjelajahi ke dalam area MSC yang baru, VLR tersambung ke MSC yang akan meminta data tentang stasion bergerak tersebut dari HLR. Nantinya, jika stasion bergerak melakukan panggilan, VLR akan mempunyai informasi yang diperlukan untuk setup panggilan tanpa harus menginterogasi HLR setiap saat. *Aunthetication Center* (AUC), menyediakan autentikasi dan enkripsi parameter untuk memverifikasi identitas pengguna dan menjamin kerahasiaan dari setiap panggilan. AUC melindungi operator jaringan dari tipe-tipe penggelapan atau kecurangan yang berbeda yang telah ditemukan saat ini di dunia selular. *Equipment Identity Register* (EIR), basis data yang berisi informasi tentang identitas dari perlengkapan mobile untuk mencegah panggilan dari pencurian, unauthorized, atau stasion bergerak yang rusak. AUC dan EIR di implementasikan sebagai node yang berdiri sendiri atau kombinasi node AUCatauEIR.

b. *Base Station System* (BSS)
Seluruh fungsi dari radio dilakukan di BSS, dimana terdiri dari BSCs dan *base transceiver stations* (BTSs) [4]. BSC menyediakan seluruh fungsi pengawasan dan hubungan fisik antara MSC dan BTS. BSC merupakan switch berkapasitas tinggi yang melakukan fungsi sebagai *handover*, data konfigurasi cell, dan kendali level daya *radio frekuensi* (RF) di *base transceiver stations*. Sejumlah BSC dapat dilayani oleh MSC. BTS menangani antarmuka radio ke mobile station. BTS adalah perlengkapan radio yang diperlukan untuk melayani setiap panggilan di masing-masing cell dalam suatu jaringan.

c. Operasi dan Support System

Operasi dan *maintenance center* (OMC) tersambung ke seluruh perlengkapan sistem switching dan ke BSC. Implementasi dari OMC disebut operasi dan support sistem (OSS). Fungsi yang penting dari OSS yaitu memberikan gambaran jaringan dan dukungan aktivitas pemeliharaan dari operasi yang berbeda dan pemeliharaan organisasi [4]. *Message Center* (MXE), adalah node yang melakukan suara, fax, dan pesan data. Khususnya, MXE menangani layanan pesan singkat, cell broadcast, voice mail, fax mail, email, dan notifikasi. *Mobile Service Node* (MSN), adalah node yang menangani layanan mobile intelligent network (IN). *Gateway Mobile Service Switching Center* (GMSC), adalah node yang digunakan untuk saling mengubungkan dua jaringan. Gateway kadang di implementasikan di dalam MSC. MSC kemudian mengacu ke GMSC. *GSM interworking unit* (GIWU), terdiri dari hardware dan software yang menyediakan antarmuka ke berbagai jaringan untuk komunikasi data. Melalui GIWU, pemakai dapat bergonta-ganti antara percakapan dan data pada saat panggilan yang sama. Perlengkapan hardware GIWU secara fisik terletak di MSCatauVLR.



Gambar 5. Elemen dasar jaringan GSM

B.2 Spesifikasi GSM [4] [12]:

Frekuensi band– range frekuensi yang dispesikasikan untuk GSM adalah 1,850 to 1,990 Mhz (mobile station ke base station). *Duplex distance* - *duplex distance* adalah 80 Mhz. Duplex distance ialah jarak antara frekuensi uplink dan downlink.

Access method– GSM memanfaatkan konsep T*ime Division Multiple Access* (TDMA), dimana beberapa panggilan berbeda memungkinkan berbagagi pembawa yang sama. Tiap panggilan di tandai slot waktu yang akurat. *Speech coder*- GSM menggunakan linear predictive coding (LPC), untuk mengurangi laju bit. LPC memberikan parameter untuk filter yang menirukan vokal. Sinyal lewat melalui filter ini, meninggalkan dibelakang sinya sisa. Percakapan di enkode pada 13 kbps.

B.3 Layanan langganan GSM [4]:

Dual-tone-multifrekuensi (DTMF) adalah gabungan nada pensinyalan yang terkadang digunakan untuk mengontrol berbagai maksud melalui jaringan telepon, seperti pengendali jarak jauh mesin penjawab. GSM mendukung penuh teknologi DTMF. *Facsimile group III* – GSM mendukung CCITT Group 3 faksimili. Sebagai standar mesin fax yang di desain untuk terhubung ke telepon menggunakan sinyal analog, pengubah khusus fax disambungkan ke pertukaran dengan mengunakan sistem GSM. Ini memungkinkan GSM tersambung fax untuk berkomunikasi dengan fax analog lainnya di jaringan. *Short*

DOI : 10.25139/inform.v3i2.1031

message services – fasilitas yang tepat dari jaringan GSM adalah *short message services*.

Sebuah pesan terdiri dari maksimum 160 karakter alphanumeric dengan beberapa keuntungan. Jika pelanggan unit mobile mematikan alatnya atau meninggalkan coverage area, pesan akan disimpan dan mengirimkan kembali saat mobile unit telah kembali menyala atau telah memasuki area yang tercakup dalam suatu jaringan. Fungsi ini menjamin suatu pesan akan diterima. *Cell broadcast* – variasi dari layanan SMS adalah fasilitas cell broadcast. Sebuah pesan dengan maksimum 93 karakter dapat di pancarkan tersebar ke seluruh pelanggan mobile pada area geografi tertentu. *Voice mail* – layanan ini sebenarnya seperti mesin penjawab didalam suatu jaringan, dimana dapat di dikendalikan oleh pelanggan. Panggilan dapat di teruskan ke pelanggan voice-mail-box dan pelanggan meng'check pesan tersebut dengan menggunakan kode keamanan pribadi. *Fax mail* – dengan layanan ini, pelanggan dapat menerima pesan fax pada mesin fax lainnya. Pesan tersebut tersimpan di service center dimana mereka dapat oleh pelanggan melalui kode keamanan pribadi yang diinginkan nomor fax. Pemetaan tower [13] untuk mengetahui kualitas layanan GSM dapat memudahkan dalam perencanaan lokasi yang belum terhubung.

B.4 Layanan Tambahan

GSM mendukung layanan-layanan tambahan secara luas dan juga mendukung layanan telepon dan data. *Call forwarding*, memungkinkan pelanggan untuk meneruskan panggilan yang masuk ke nomor lain jika mobile unit yang tidak dapat dicapai, jika sedang sibuk, tidak ada balasan, atau jika fasilitas panggilan diteruskan di gunakan pada saat keadaan tak terkondisi. B*arring of outgoing calls*, memungkinkan pelanggan untuk mencegah seluruh panggilan keluar. *Barring of incoming calls* untuk mencegah panggilan masuk. Terdapat dua kondisi: baring seluruh panggilan masuk dan baring seluruh panggilan masuk bila termasuk roaming. *Advice of charge (aoc)*, memungkinkan pelanggan memperkirakan biaya panggilan. Terdapat dua tipe informasi aoc: yang pertama memungkinkan pelanggan memmperkirakan tagihan biaya dan yang kedua dapat digunakan untuk pengisian. Aoc untuk panggilan berupa data sebagai basis menghitung waktu. *Call hold*, memungkinakan pelanggan untuk menyela panggilan dan secara berurutan membuat panggilan kembali. Layanan ini hanya dapat dipakai ke telepon biasa. *Call waiting*, memungkinkan pelanggan untuk diberitahukan adanya panggilan masuk ketika sedang terjadi percakapan. Pelanggan dapat menjawab, menolak, atau menyisihkan panggilan yang datang tersebut. Call wating hanya dapat dipakai ke seluruh layanan telekomunikasi gsm dengan menggunakan koneksi circuit-switched. *Multiparty service*, memungkinkan pelanggan untuk melakukan percakapan multyparty – percakapan yang simultan antara 3 dan 6 pelanggan lainnya. Layanan ini hanya dapat dipakai untuk telepon biasa. *Calling line identification presentationataurestriction*, menyediakan called party dengan layanan isdn secara terpadu. Pembatasan layanan memungkinkan party yang memanggil untuk membatasi presentasi. *Closed user gorups* (cugs), merupakan group dari pelanggan yang capable jika memanggil group mereka sendiri dan nomor-nomor tertentu.

B.5 Aspek Keamanan yang disediakan GSM [4] [11]:

Autentifikasi pengguna, yaitu kemampuan telepon selular untuk membuktikan apakah yang melakukan akses adalah pengguna yang sah. Kerahasiaan data dan sinyal, yaitu proses mengenkripsi pesan dan data yang di transmisikan. Kerahasiaan pengguna sewaktu jaringan butuh identitas pelanggan atau selama proses autentifikasi IMSI (International Mobile Subscribe Identity) yang unik tidak dalam bentuk plainteks (sudah terenkripsi)

V. KESIMPULAN

Dari segi teknologi, CDMA menggunakan teknologi Broadband CDMA merupakan teknologi spektrum lanjutan yang digunakan untuk kepentingan komersil dan dapat memberikan kelebihan kualitas suara yang tinggi, karakteristik fade dan performansi indoor (dalam ruangan) yang sangat baik serta dinamika rata-rata data yang baik. Sedangkan GSM menggunakan teknologi akses TDMA *(Time Division Multiple Access)*, yang mana merupakan sebuah teknologi digital dengan membagi-bagi spektrum yang tersedia kepada sejumlah channel diskrit yang tetap, meskipun masing-masing channel merepresentasikan time slot yang tetap daripada band frekunesi yang tetap, sehingga komunikasi dapat berjalan stabil atau konstan. Pada segi jaringan CDMA dapat dimodelkan secara sederhana menggunakan spectrum tersebar runtun langsung (DS-CDMA). Pemodelan di sini dibatasi untuk kanal maju (*forward channel*) atau *downlink*, yaitu transmisi dari BTS ke MS. Model ini dibedakan menjadi bagian Pengirim dan Penerima. Sedangkan Jaringan GSM dibagi menjadi tiga sistem utama: sistem *switching* (SS), sistem *base station* (BSS), dan sistem operasi dan support (OSS). Pada aspek keamanan dapat GSM menggunakan algoritma A3 dan A8 untuk proses autentikasi, yaitu proses pengenalan identitas pelanggan, yang terjadi pada MS (*Mobile Station*) dan AUC (*Authentication Centre*) Sedangkan algoritma A5 digunakan dalam proses pengiriman informasi pada link radio antara MS dengan BTS (*Base Transceiver Station*). Namun pada sistem pengamanan dengan menggunakan algoritma ini ditemukan kelemahan-kelemahan yang memungkinkan terjadinya penyadapan data ataupun penipuan identitas pelanggan. Sedangkan CDMA menawarkan aspek keamanan jaringan dengan mengembangkan algoritma enkripsi. Untuk teknik enkripsi digunakan algoritma Rijndael yang aman dan sangat cepat.

REFERENSI

[1] S. Neeraja and G. Sasibhushana Rao, “Comparative study on handoff algorithms for GSM and CDMA cellular networks,” *Int. J. Electr. Comput. Eng.*, 2017.

[2] O. O. Fagbohun, “Comparative studies on 3G,4G and 5G wireless technology,” *IOSR J. Electron. Commun. Eng. Ver. I*, 2014.

[3] J.-Z. Sun, J. Sauvola, and D. Howie, “Features in Future: 4G Visions

DOI : 10.25139/inform.v3i2.1031

From a Technical Perspective," in *GLOBECOM'01. IEEE Global Telecommunications Conference*, 2001.
[4] I. Arnomo, "Studi Perbandingan Teknologi Telekomunikasi Seluler CDMA (Code Division Multiple Access) dan GSM (Global System for Mobile communication)," Universitas Narotama, Surabaya, 2009.
[5] S. Chen and J. Zhao, "The requirements, challenges, and technologies for 5G of terrestrial mobile telecommunication," *IEEE Commun. Mag.*, 2014.
[6] K. G. S. Venkatesan, "Comparison of CDMA and GSM mobile technology," *Middle - East J. Sci. Res.*, 2013.
[7] R. Sustika, "Analisis Aspek-Aspek Perencanaan BTS pada Sistem Telekomunikasi Selular Berbasis CDMA," *INKOM*, vol. 1, no. 1, pp. 31–38, 2007.
[8] L. O. NUR, "ANALISA UNJUK KERJA CDMA 2000 1X PADA KANAL AWGN DAN RAYLEIGH FADING," *Maj. Ilm. UNIKOM*, vol. 7, no. 1, pp. 125–136.
[9] R. R. K. Dewanti, T. Maulana, and A. Aminulloh, "SISTEM KOMUNIKASI CDMA."
[10] S. U. Wicaksono, "KAJIAN SISTEM KEAMANAN JARINGAN CDMA."
[11] N. Sharma and M. Yadav, "A Review Paper on GSM Security and Encryption," in *National Conference on Innovations in Micro-electronics, Signal Processing and Communication Technologies*, 2016, pp. 88–90.
[12] E. Ihsanto and T. W. Riyanto, "DISAIN DAN IMPLEMENTASI SISTEM PENJEJAK POSISI KENDARAAN DENGAN GPS VIA SMS," *J. Ilm. SINERGI*, 2013.
[13] A. V. Vitianingsih and M. S. Reza, "REKAYASA SISTEM INFORMASI GEOGRAFIS (SIG) UNTUK PEMETAAN LOKASI TOWER JARINGAN TELEPON SELULER DALAM BENTUK WEBMAP DI JAWA TIMUR," *J. Ilm. Ilmu Komput.*, vol. 8, no. 2, pp. 201–206, 2012.

DOI : 10.25139/inform.v3i2.1031