

Makalah
Kajian Sistem Keamanan Jaringan 3G dan
CDMA 2000 1x EV-DV
(Tugas Matakuliah Keamanan Sistem Lanjut EC 7010)

Oleh:
Jenny Evelin Palunsu
NIM 23203111



Program Magister Teknik Elektro
Bidang Khusus Teknologi Informasi Dikmenjur
INSTITUT TEKNOLOGI BANDUNG
2004

KATA PENGANTAR

Dengan selesainya tulisan ini, maka patutlah penulis mengungkapkan rasa syukur kepada Tuhan Yang Maha Esa atas karunia dan berkatNya selama proses pengumpulan data dan informasi serta penulisan makalah ini. Penulis menyampaikan rasa terimakasih kepada Bapak Dr. Ir. Budi Raharjo M.Sc. sebagai pembimbing matakuliah EC 7010 Keamanan Sistem Lanjut yang telah memberikan kesempatan kepada penulis untuk melakukan pendalaman terhadap terhadap topik keamanan jaringan serta salah satu sistim keamanan didalam generasi tersebut. Judul yang diambil yakni '**Sistem Keamanan Jaringan 3G dan CDMA 2000 1x EV-DV**'. Harapan penulis semoga tulisan ini dapat bermanfaat bagi rekan-rekan mahasiswa Departemen Elektro Bidang Khusus Teknologi Informasi Program Pasca Sarjana Institut Teknologi Bandung Angkatan 2003 serta seluruh insan yang berkecimpung dalam pengembangan teknologi informasi. Semoga ada manfaatnya dan terimakasih.

Bandung, 10 Desember 2004
Penulis

ABSTRAKSI

Jenny Evelin Palunsu

NIM 232 00 311

Teknologi Informasi, Departemen Elektro

Institut Teknologi Bandung, Indonesia

jpalsu@yahoo.com

Sistem keamanan pada suatu jaringan komunikasi menjadi salah satu hal penting untuk berhasilnya sebuah sistem informasi. Tujuan diciptakannya jaringan komunikasi generasi ketiga (3G) adalah untuk menyediakan standar tertentu yang dapat melingkupi kebutuhan-kebutuhan aplikasi-aplikasi nirkabel yang sangat luas variasinya serta untuk menyediakan akses yang bersifat global. Berbagai perkembangan teknologi jaringan telah dikembangkan antara lain UMTS, EDGE, CDMA, WCDMA dan Standar IEEE 802.20. Pada setiap perkembangan dipersyaratkan pengembangan sistem keamanan juga. Pada teknologi CDMA 1x EV-DV yang merupakan bagian dari CDMA 2000 mengimplementasikan sistem keamanan yakni enkripsi dan otentifikasi. Pada teknik enkripsi digunakan algoritma Rijndael (*Rijndael Encryption Algorithm*) yang aman dan sangat cepat dan hanya memungkinkan penggunaan ukuran kunci 128, 192 and 256-bit. Sedangkan pada otentifikasi menggunakan prosedur *Unique Challenge Procedure* dimana *base station* mengenerate 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*".

Kata Kunci:

Sistim Keamanan, CDMA 2000 1x EV-DV, Enkripsi, Otentifikasi

DAFTAR ISI

KATA PENGANTAR	i
ABSTRAKSI	ii
DAFTAR ISI	iii
DAFTAR GAMBAR	iv
DAFTAR TABEL	v
BAB I PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Tujuan.....	1
1.3. Ruang Lingkup.....	2
BAB II SISTIM KEAMANAN JARINGAN 3G	3
2.1. Latar Belakang.....	3
2.2. Ciri-ciri Sistim Komunikasi 3G.....	3
2.3. Jenis Sistim Keamanan 3G.....	3
2.3.1. UMTS.....	4
2.3.2. EDGE.....	4
2.3.3. CDMA2000.....	4
2.3.4. WCDMA.....	5
2.3.5. IEEE.802.20.....	6
2.4. Prinsip-prinsip Sistim Keamanan 3G.....	6
2.5. Tujuan Sistim Keamanan 3G.....	6
2.6. Peran Sistim Keamanan 3G.....	7
2.7. Elemen Sistim Keamanan 2G Dipertahankan 3G.....	7
2.8. Kelemahan Sistim Keamanan 2G Diperbaiki untuk 3G.....	8
BAB III SISTEM KOMUNIKASI JARINGAN 1xEV-DV	9
3.1. Latar Belakang.....	9
3.2. Konsep Kunci 1xEV-DV.....	9
3.2.1. Modulasi dan Coding yang adaptif (Adaptive Modulation dan Coding).....	9
3.2.2. Penjadwalan Cepat (Fast Scheduling).....	9
3.2.3. Multi-User Diversity.....	10
3.2.4. Macro Diversity.....	10
3.3. Konsumsi Power (Power Consumption).....	10
3.4. Quality of Service dalam Sistim 1xEV-DV.....	11
3.5. Persyaratan untuk 1x EV-DV.....	11
BAB III SISTIM KEAMANAN 1xEV-DV	12
4.1. Enkripsi dan Otentifikasi dalam sistim 1xEV-DV.....	13
4.1.1. Enkripsi.....	13
4.1.2. Otentifikasi (Authentication).....	14
4.1.3. Voice, Signaling, and Data Privacy.....	16
BAB IV PENUTUP	17
Daftar Pustaka	18

DAFTAR GAMBAR

Gambar 1. Jalur Evolusi CDMA 2000.....	5
Gambar 2. Adaptif Modulasi dan Coding.....	9
Gambar 3. Enkripsi dalam 1xEV-DV.....	13
Gambar 4. Mekanisme Otentifikasi dan Enkripsi.....	15

DAFTAR TABEL

Tabel 1. Klas QoS (QoS Classes)	11
Tabel 2. Persyaratan 1xEV-DV.....	11
Tabel 3. Field Enkripsi	14

BAB I PENDAHULUAN

1.1. Latar Belakang

Sistem keamanan pada suatu jaringan menjadi salah satu hal penting sebuah sistem informasi. Keamanan jaringan biasanya tidak terlalu diperhatikan oleh pemilik sistem informasi ataupun pengelolanya. Keamanan jaringan biasanya menjadi prioritas terakhir untuk diperhatikan, bahkan sekalipun terjadi penurunan kemampuan kerja komputer. Jika hal tersebut terjadi pemilik pada umumnya akan mengurangi aspek keamanan atau bahkan aspek keamanan akan ditiadakan untuk tujuan mengurangi beban kerja komputer. Sebagai konsekuensi peniadaan sistem keamanan maka kemungkinan informasi penting dan rahasia dapat diketahui oleh pihak lain. Hal buruk lain yang dapat terjadi misalnya informasi penting tersebut dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mengeruk keuntungan sendiri bahkan dapat merusak kinerja pemilik informasi. Kejahatan seperti itu biasanya dilakukan langsung terhadap sistem keamanan yang bersifat fisik, sistem keamanan yang berhubungan dengan personal, keamanan data dan media serta teknik komunikasi dan keamanan operasi.

Sistem komunikasi nirkabel generasi ketiga atau sering disingkat 3G adalah hasil pengembangan generasi kedua. Sistem ini disebut dengan nama sistem *Broadband Mobile Multimedia* yang berbasis UMTS. Tujuan jaringan komunikasi 3G yakni untuk menyediakan seperangkat standar tertentu yang dapat memenuhi kebutuhan aplikasi-aplikasi nirkabel cukup luas variasinya serta untuk menyediakan akses secara global. Sistem komunikasi nirkabel membutuhkan implementasi sistem keamanan yang sesuai dengan ciri dan arsitektur masing-masing. Pada makalah akan dikaji khususnya sistem keamanan untuk teknologi komunikasi generasi ketiga (3G) dan lebih difokuskan lagi pada CDMA 2000 1 x EV-DV. Maka judul makalah ini adalah '**Sistem Keamanan Jaringan 3G dan CDMA 2000 1x EV-DV**'.

1.2. Tujuan

Tujuan penulisan makalah ini adalah:

- Mengetahui ciri-ciri dan jenis teknologi jaringan nirkabel pada generasi ketiga (3G);
- Mengetahui elemen sistem keamanan 2G yang dapat dipertahankan;
- Mengetahui tujuan, prinsip, peran sistem keamanan, serta arsitektur 3G;
- Mengkaji sistem komunikasi dan keamanan CDMA 2000 1x EV-DV.

1.3. Ruang Lingkup

Ruang lingkup makalah ini meliputi antara lain: ciri-ciri sistem komunikasi 3G, jenis telekomunikasi 3G (UMTS, EDGE, CDMA 2000, WCDMA, IEEE.802.20), elemen sistem keamanan generasi kedua yang perlu dipertahankan, kelemahan sistem keamanan pada generasi kedua yang perlu diperbaiki, tujuan sistem keamanan 3G, prinsip-prinsip sistem keamanan 3G, peran sistem keamanan 3G. Selain itu juga akan dilakukan pengkajian terhadap sistem komunikasi CDMA 2000 1x EV-DV dimana akan dilihat konsep kunci dari sistem ini, persyaratan 1x EV-DV, konsumsi *power*, *Quality of Service* dalam sistem 1xEV-DV, *interface* udara. Selanjutnya dilakukan pengkajian terhadap sistem keamanan yang digunakan pada CDMA2000 1x EV-DV yang meliputi enkripsi dan otentifikasi.

BAB II

SISTEM KEAMANAN JARINGAN 3G

2.1. Latar Belakang

Sistem komunikasi jaringan nirkabel generasi ketiga atau sering disebut jaringan 3G merupakan pengembangan dari sistem komunikasi jaringan nirkabel bergerak dari generasi kedua. Sistem ini dikenal dengan nama sistem *Broadband Mobile Multimedia* yang berbasis *Universal Mobile Telecommunication System* (UMTS). Tujuan diciptakannya jaringan komunikasi 3G yakni untuk menyediakan standar tertentu yang dapat melingkupi kebutuhan-kebutuhan aplikasi-aplikasi nirkabel yang sangat luas variasinya serta untuk menyediakan akses yang bersifat global.

2.2. Ciri-ciri Sistem Komunikasi 3G

Sistem komunikasi nirkabel 3G ini memiliki ciri-ciri sebagai berikut.

- memiliki standar yang bersifat global atau mendunia;
- memiliki kesesuaian atau kompatibilitas layanan dengan jaringan kabel lain;
- memiliki kualitas yang tinggi baik suara, data, maupun gambar;
- memiliki pita frekuensi yang berlaku umum di seluruh dunia;
- memiliki kemampuan penjelajahan ke seluruh dunia;
- memiliki bentuk komunikasi yang bersifat multimedia baik layanan maupun piranti penggunaannya;
- memiliki spektrum yang efisien;
- memiliki kemampuan untuk evolusi ke sistem nirkabel generasi berikutnya;
- memiliki laju data paket 2 Mbps perangkat yang diam di tempat atau terminal, 384 kbps untuk kecepatan orang berjalan serta 144 kbps untuk kecepatan orang berkendara.

2.3. Jenis Sistem Komunikasi 3G

Sistem komunikasi 3G menggunakan jaringan layanan digital terpadu berpita lebar (B-ISDN) untuk mengakses jaringan-jaringan informasi seperti internet, basis data publik maupun data pribadi lainnya. Selain itu jaringan ini juga dioperasikan di berbagai wilayah, yang penduduknya padat maupun jarang serta melayani pengguna baik yang diam di tempat (*steady/station*), maupun yang bergerak dalam kendaraan berkecepatan tinggi (*mobile*). Istilah *personal communication system* (PCS) dan *personal communication network* (PCN) digunakan untuk menyatakan munculnya sistem generasi ketiga untuk perangkat-perangkat genggam khususnya ponsel. Nama lain dari teknologi tersebut yakni *future public land mobile*

telecommunication systems dimana penggunaan di seluruh dunia dikenal dengan nama IMT 2000 dan UMTS. Berikut ini adalah penjelasan tentang beberapa sistem komunikasi yang termasuk dalam sistem komunikasi jaringan 3G.

2.3.1.UMTS

UMTS adalah singkatan dari *universal mobile telecommunication system* merupakan suatu sistem komunikasi bergerak generasi ketiga yang diharapkan mampu memberi layanan sampai 2 Mbps dan pada frekuensi sekitar 2 GHz. Sistem UMTS yang diusulkan dibangun dari infrastruktur sistem-sistem bergerak (*mobile*) yang telah ada seperti *global system for mobile communication* (GSM), *advance mobile phone system* (AMPS), *personal communication system* (PCS) dan lain-lain yang berevolusi menuju UMTS. Forum UMTS memperkirakan komunikasi multimedia berbasis data akan menyumbang sekitar 60% pada lalu lintas komunikasi dalam jaringan komunikasi bergerak generasi ketiga.

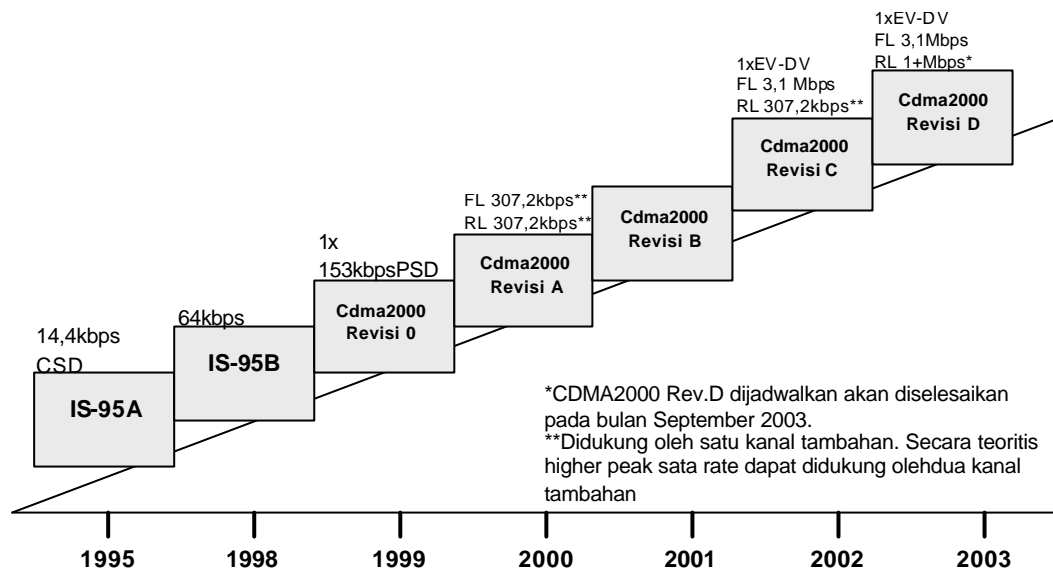
2.3.2.EDGE

Enhanced data rates for global evolution (EDGE) merupakan hasil pengembangan dari GPRS generasi 2,5. EDGE memungkinkan operator menyediakan layanan data pada kecepatan sampai 384 kbps. EDGE merupakan salah satu standar nirkabel data yang diimplementasikan pada jaringan selular GSM serta merupakan tahapan lanjutan evolusi menuju *mobile multi media communication*. Sistem ini memungkinkan jaringan memiliki kecepatan transmisi data sampai 126 kbps dan menjadi teknologi transmisi data paling cepat. Menurut *GSM World Association*, EDGE juga dapat mencapai kecepatan hingga 473,8 kbps. Selain peningkatan kecepatan pengiriman data, sistem ini juga dapat meningkatkan kapasitas transmisi data. Kemampuan EDGE mencapai 34 kali kecepatan akses jalur kabel telepon (sekitar 30-40 kbps) dan hampir 2 kali lipat kecepatan cdma 2000 1x (sekitar 70-80 kbps).

2.3.3.CDMA 2000

Teknologi *Code Division Multiple Access* (CDMA) merupakan salah satu alternatif dari arsitektur GSM seluler. Kedua tipe jaringan tersebut membuat transisi ke sistem generasi ketiga (3G) dengan menawarkan layanan kapasitas yang lebih dan layanan data. Teknologi CDMA mendesak agar sistem pada 3G seperti cdma2000 1x dan cdma2000 1x EV-DO segera diimplementasikan. Perkembangan sistem komunikasi jaringan cdma2000 melalui 1x dikenal dengan nama CDMA2000 1xEV. Sistem 1xEV akan dibagi dalam dua step yakni: ¹⁾ 1xEV-DO dan ²⁾ 1xEV-DV. Sistem 1xEV-DO adalah singkatan dari 1x *evolution data only*

sedangkan 1xEV-DV adalah singkatan dari 1x *evolution data and voice*. Gambar 1 menunjukkan perjalanan pengembangan atau evolusi dari sistem CDMA 2000.



Gambar 1. Jalur Evolusi CDMA 2000

CDMA 2000 1xEV-DO dan 1xEV-DV merupakan perkembangan dari cdma2000 1xEV dengan maksud untuk memberikan layanan yang lebih baik pada cdma2000 menggunakan standar 1.25 MHz. Sistem 1xEV-DO sudah dapat digunakan oleh operator cdma2000 sekitar tahun 2002, dan akan menyediakan kapasitas data lebih besar pada sistem 1x. Sistem 1xEV-DO mensyaratkan pengantaran data yang terpisah, namun mampu melakukan hand-off ke pengantar 1x jika layanan data dan suara secara simultan dibutuhkan. Melalui pengalokasian pengantaran data secara terpisah, operator akan mampu mengantar data pada patokan puncak sampai 2 Mbps ke pelanggan. Sistem cdma2000 1xEV-DV akan membuat layanan data dan suara untuk cdma2000 menjadi satu. Sistem 1xEV-DV akan memberikan kecepatan pengantaran data dan suara yang tinggi secara bergantian juga mengantar layanan paket secara *realtime*.

2.3.4. WCDMA

WCDMA adalah singkatan dari *Wideband CDMA* yang diperkenalkan secara umum pada tahun 2001-2002 di Jepang dan selanjutnya memasuki daratan Eropa. Di Amerika Serikat beberapa alternatif sistem jaringan komunikasi 3G dapat diperoleh operator GSM dan TDMA yang berkembang ke arah EDGE dengan WCDMA. WCDMA merupakan sistem operasi generasi ketiga (3G) yang beroperasi pada *bandwidth* 5 MHz. Rata-rata data sampai 384 kbps untuk area jangkauan yang cukup luas. Variasi penyebaran dan operasi multi kode telah

digunakan untuk mendukung banyaknya perbedaan batasan *access radio*. Perbedaan kelas layanan telah didukung oleh *Quality of Service (QoS)*.

2.3.5.IEEE.802.20

Standar IEEE 802.20 merupakan suatu standar baru yang dapat merubah arah jaringan nirkabel. Standar IEEE 802.20 ditujukan untuk *local and metropolitan area networks* dengan spesifikasi antara lain menawarkan perluasan *range* untuk *broadband wireless* meskipun tidak kompatibel dengan layanan seluler yang ada. Standar 802.20 merupakan *packet-based system* yang optimal untuk transmisi data. Spesifikasi layer fisik dan layer *medium access control (MAC)* dari *interface* udara untuk *interoperable mobile broadband wireless access system* dioperasikan dalam *band* yang terlisensi dibawah 3.5 GHz. Pengoptimalan untuk IP transfer data, dengan rata-rata puncak data per pengguna pada perpanjangan dari 1 Mbps. Hal ini mendukung pengelompokan *vehicular mobility* sampai pada 250 km/h pada lingkungan MAN dengan harapan terjadi efisiensi, mempertahankan rata-rata pengguna data dan jumlah pengguna aktif yang secara signifikan lebih tinggi dibanding pencapaian melalui *mobile system* yang telah ada.

2.4. Prinsip-prinsip Sistim Keamanan 3G

Terdapat tiga prinsip kunci pada sistim keamanan jaringan komunikasi generasi ketiga (3G) yakni:

- sistim keamanan 3G dibangun pada sistim keamanan generasi kedua. Elemen-elemen sistim keamanan dalam GSM dan sistem yang lain pada generasi kedua yang telah teruji kuat penting untuk diadopsi untuk sistim keamanan 3G;
- sistim keamanan 3G memperbaiki sistim keamanan generasi kedua yang artinya bahwa sistim keamanan 3G memusatkan perhatian dan melakukan koreksi terhadap kekurangan pada generasi kedua;
- sistim keamanan 3G menawarkan *feature* sistim keamanan dan layanan baru.

2.5. Tujuan Sistim Keamanan 3G

Terdapat beberapa tujuan dari sistim keamanan jaringan komunikasi generasi ketiga (3G) antara lain:

- untuk menjamin bahwa informasi melalui atau yang berhubungan ke pengguna terlindungi secara seimbang dari kesalahan penggunaan atau kejahatan lain;
- untuk menjamin perlindungan terhadap sumber daya dan layanan yang diberikan melalui jaringan maupun lingkungan rumah secara seimbang terhadap kesalahan penggunaan;

- untuk menjamin standarisasi layanan sehingga memungkinkan kompatibel dengan dunia luas;
- untuk menjamin keamanan terstandar secara seimbang untuk menjamin interoperabilitas secara dunia luas serta *roaming* antara layanan jaringan yang berbeda;
- untuk menjamin tingkat perlindungan lebih baik bagi pengguna dan pemberi layanan baik jaringan *fixed* maupun yang *mobile* (termasuk GSM);
- untuk menjamin perluasan dan peningkatan implementasi layanan keamanan 3GPP dengan mekanisme sebagaimana dipersyaratkan oleh usaha layanan.

2.6. Peran Sistim Keamanan 3G

Peran sistim keamanan pada jaringan komunikasi 3G yakni merupakan usaha memungkinkan sistim keamanan itu sendiri untuk diidentifikasi dan berhubungan dengan persyaratan keamanan yang dibangun secara sistematis. Peran sistim keamanan direpresentasikan dari entitas yang logis, pelaku bisnis, manusia dan mesin fisik. Terdapat beberapa kelompok yang terlibat dalam penentuan serta menggunakan sistim keamanan 3G dikelompokkan dalam satu entitas. Sebagai contoh perusahaan tertentu mungkin melakukan aksi untuk sistim keamanan lingkungan rumah dan sistim keamanan layanan jaringan. Maka hal tersebut diasumsikan sama dengan seseorang yang ingin menjadi *subscriber* dan *user*. Dengan demikian domain yang ada untuk suatu sistim keamanan lingkungan rumah maupun layanan jaringan yakni domain *user* dan domain infrastruktur.

2.7. Elemen Sistim Keamanan 2G Dipertahankan 3G

Elemen-elemen dari sistim keamanan 2G yang dipertahankan pada sistim keamanan 3G antara lain:

- *Authentication* pengguna untuk akses layanan yakni jika terjadi ketidak-seimbangan algoritma yang mana terkait dengan otentifikasi;
- *Encryption interface radio*. Kekuatan dari enkripsi menjadi lebih besar bila dibandingkan dengan yang digunakan pada sistim keamanan generasi kedua (kekuatan dimaksud adalah kombinasi panjang kunci dan desain algoritma);
- *Confidential identity subscriber* pada *radio interface*. SIM yang *removable* dan *hardware module* sistim keamanan yang memiliki *feature* misalnya dapat dikelola oleh operator jaringan; dan independen dari terminal sebagaimana fungsi keamanan;
- Aplikasi SIM, *feature* keamanan menyediakan jaminan kanal layer aplikasi antara SIM dan server jaringan rumah;
- *Feature* operasi sistim keamanan sifatnya independen untuk pengguna, artinya bahwa pengguna tidak harus melakukan apapun untuk mengoperasikan *feature* keamanan.

2.8. Kelemahan Sistem Keamanan 2G Diperbaiki untuk 3G

Kelemahan-kelemahan pada generasi kedua *GSM* antara lain:

- Penyerang yang aktif menggunakan “kekeliruan *BTS*” mungkin terjadi;
- *Cipher key* dan otentifikasi data ditransmisikan secara jelas di antara dan di dalam jaringan;
- Enkripsi tidak diperluas untuk hasil inti jaringan dalam transmisi *cleartext* dari pengguna dan sinyal data melewati *links* gelombang mikro (di *GSM*, dari *BTS* ke *BSC*);
- *User authentication* yang menggunakan *cipher key* yang dikembangkan terlebih dahulu seperti *RAND*, *SRES* dan *A3/8* tidak ada lagi;
- Integritas data tidak disediakan. Integritas data akan gagal menghadapi penyerangan *BTS* tertentu yang keliru dan, tanpa adanya enkripsi, menyediakan perlindungan terhadap kanal *hijack*;
- *IMEI* merupakan identitas yang tidak terjamin dan seharusnya disediakan;
- Sistem pada generasi kedua tidak memiliki fleksibilitas untuk meningkatkan atau memperbaiki fungsi keamanan setiap waktu.

BAB III

SISTEM KOMUNIKASI JARINGAN 1xEV-DV

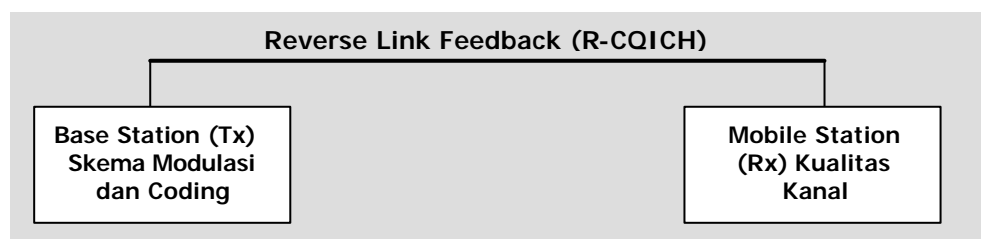
3.1. Latar Belakang

Sistem 1xEV-DV adalah salah satu sistem jaringan komunikasi yang berbasis CDMA pada 3G dengan interface udara. Sistem 1xEV-DV merupakan fase kedua dari perkembangan CDMA 2000 yang menawarkan kompatibilitas yang lengkap sebagaimana dimiliki CDMA 2000. Sistem 1xEV-DV juga kompatibel dengan standar jaringan inti dari ANSI-41. Entitas utama dalam arsitektur jaringan 3G yakni *Radio Access Network (RAN)* dan *Core Network*. *Terminal Mobile* dalam RAN berkomunikasi dengan *base station* dari *point contact* mereka untuk jaringan. Komunikasi nirkabel yang menghubungkan antar terminal-terminal dan BS menggunakan *interface* udara juga dikenal dengan *Um interface*. Jaringan inti *circuit-switched* berakhir di PSTN, sedangkan jaringan inti *packet-switched* berakhir di internet. Sistem 1xEV-DV tidak membawa dampak ke jaringan inti dari CDMA 2000.

3.2. Konsep Kunci 1xEV-DV

3.2.1. Modulasi dan Coding yang adaptif (*Adaptive Modulation dan Coding*)

Berdasarkan kondisi kanal rata-rata pengalaman pengguna bahwa *Modulation* fleksibel dan skema *Coding* telah dipilih untuk layanan terhadap pelanggan yang bervariasi. Kondisi kanal secara kontinyu berkomunikasi melalui mobile station menggunakan FPDCH melalui R-CQICH. Hal ini memungkinkan adaptif *rate operation*.



Gambar 2. Adaptif Modulasi dan Coding

3.2.2. Penjadwalan Cepat (*Fast Scheduling*)

Penjadwalan cepat untuk paket data mengontrol alokasi kanal untuk pengguna dan menentukan sifat secara umum dari sistem. Penjadwal (*scheduler*) mentransmisikan data ke pengguna dengan kondisi kanal terbaik setiap waktu, dan memungkinkan data rate tertinggi setiap saat. Hal tersebut dimaksimalkan dalam *throughput*.

3.2.3. Multi-User Diversity

Sistim CDMA memiliki *bandwidth* yang cukup signifikan untuk pengiriman paket data meski kondisi kanal lemah. Dengan teknik *adaptive rate*, sistim 1xEV-DV mampu mencapai tingkat efisien *multiplexing* diantara berbagai pengguna. Sistim 1xEV-DV mendukung *packet-based* TDM dan CDM. Pada TDM, *base station* mentransmisikan paket-paket yang pendek ke pengguna sebanyak satu paket dalam satu satuan waktu dengan menggunakan segala kemungkinan sumber daya udara (*power* dan *code space*), serta pada *maximum data rate* kondisi kanal penerima yang memungkinkan.

3.2.4. Macro Diversity

Setiap terminal 1xEV-DV secara konstan memonitor kanal pilot yang menerima dari berbagai *base station* yang berbeda. Terminal tersebut berkomunikasi dengan transmisi *base station* yang berkaitan dengan pilot terkuat yang menerima. Dengan cara ini terminal akan mengidentifikasi dari *base station* mana dia akan menerima sinyal. Hal ini menolong dalam mengurangi beban pada pengontrol jaringan radio. Selain itu juga cukup menolong dalam mengkonservasi sumber daya udara dalam situasi *handoff* yang *soft* yang mana didalamnya *multiple base station* mengirimkan *frame* yang sama ke terminal tertentu yang sedang mengerjakan dengan *soft handoff*.

3.3. Konsumsi Power (*Power Consumption*)

Tanpa melihat teknologi RF, pengiriman *high data rate* mensyaratkan *power* yang lebih besar, dan oleh sebab itu akan menghasilkan pembuangan *power* dari baterai. Untuk mengurangi konsumsi *power*, maka apabila bit yang dikirimkan sedikit (misalnya pesan singkat atau *short message*) maka hanya akan membutuhkan *power* yang sedikit pula. Jika bit yang dikirimkan lebih banyak seperti *video clip*, maka membutuhkan *power* lebih besar. Jadi, terminal 1xEV-DV menjadi lebih efisien, dimana dalam pengalokasian *power* RF hanya sesuai dengan yang dibutuhkan untuk mentransmisikan bit. Selain itu, sistim 1xEV-DV juga mendukung *Discontinuous Transmission* (DTX) dimana *Base station* atau *mobile station* memindahkan (*switches*) transmiternya menjadi tidak aktif (*off*) apabila tidak ada data yang harus dikirimkan dan akan segera mengaktifkan (*on*) apabila ada data yang sedang dalam antrian untuk dikirim.

3.4. *Quality of Service* dalam Sistim 1xEV-DV

Quality of Service (QoS) sistim 1xEV-DV memberi kemampuan kepada pengguna maupun operator jaringan secara langsung dalam menyediakan layanan yang berbasis perbedaan (*differentiated*) berdasarkan aplikasi yang dibutuhkan pengguna. Terdapat empat perbedaan

QoS terhadap kelas layanan sebagaimana ditunjukkan pada berikut dimana mirip dengan pembagian kelas pada lalu lintas UMTS.

Tabel 1. Klas QoS (QoS Classes)

Klas	Penjelasan
Klas Percakapan (<i>Conversational class</i>)	Dua jalur, rendah penundaan, kehilangan data rate rendah, sensitif terhadap variasi penundaan, misalnya <i>video conferencing</i>).
Klas Streaming (<i>Streaming class</i>)	Sama dengan conversational, satu jalur, sensitifitas rendah terhadap penundaan, kemungkinan mensyaratkan bandwidth tinggi, misalnya pengambilan event olahraga secara live maupun event lainnya.
Klas Interaktif (<i>Interactive class</i>)	Dua jalur, <i>bursty</i> , mensyaratkan <i>bandwidth</i> bervariasi, penundaan moderat, koreksi kehilangan <i>data rate</i> secara moderat untuk sebagian, misalnya <i>WWW, Email, Telnet</i> .
Klas Latar Belakang (<i>Background class</i>)	Toleransi tinggi terhadap penundaan dan kehilangan <i>data rate</i> , memiliki variasi <i>bandwidth</i> , misalnya latar belakang <i>download file</i> .

Perbedaan tingkatan layanan yang terkait dengan penjelasan diatas termasuk antara lain:

- *Bandwidth*: kemampuan sistim untuk menyediakan kapasitas yang diperlukan untuk mendukung persyaratan *throughput* untuk aplikasi pengguna.
- *Latency (delay)*: Jumlah waktu yang digunakan untuk mengirinkan paket dari node pengirim ke node penerima.
- *Jitter*: Ukuran variasi penundaan antara kedatangan paket pada penerima.
- *Traffic loss*: Pembuangan packets karena kesalahan (*error*) atau kebakaran jaringan.

3.5. Persyaratan untuk 1x EV-DV

Persyaratan untuk 1x EV-DV 3GPP2 terdapat pada dokumen “S.R0026 *High-Speed Data Enhancements* untuk cdma2000 1x – *Integrated Data and Voice*”. Beberapa persyaratan utama 1xEV-DV tersebut antara lain:

Tabel 2. Persyaratan 1xEV-DV

Persyaratan	Catatan
Kompatibel dengan jaringan ANSI-41	
Relatif terhadap CDMA 2000, paling sedikit dua kali jumlah suara panggilan untuk kanal radio tunggal (<i>single</i>), untuk konfigurasi antena <i>base station</i> yang sama dan menggunakan <i>vocoder</i> yang sama	Kapasitas suara dari CDMA 2000 dipertahankan dalam 1xEV-DV
Paling sedikit 2.4 Mbps pada batas kanal <i>forward</i> ketika layanan hanya lalu lintas paket data untuk pengguna <i>outdoor</i> , lingkungan <i>vehicular</i> kecepatan tinggi.	3.09 Mbps didukung pada F-PDCH
Paling sedikit 1,25 Mbps pada batas kanal balik jika hanya melayani lalu lintas paket data untuk pengguna <i>outdoor</i> , lingkungan <i>vehicular</i> kecepatan tinggi.	Puncak data rate pada hubungan balik adalah 451.2 kbps

Persyaratan	Catatan
Paling sedikit 600 kbps pada batas kanal pengiriman jika hanya melayani lalu lintas paket data untuk pengguna <i>outdoor</i> , lingkungan <i>vehicular</i> kecepatan tinggi.	Rata-rata data rate 1.7 Mbps didukung pada kanal batas pengiriman
1xEV-DV seharusnya dioperasikan dengan 3x radio konfigurasi	1xEV-DV dapat dengan mudah dikembangkan untuk mengoperasikan dalam 3x mode dibawah <i>framework</i> sistim yang ada.
<i>Handoff</i> layanan suara dan data antara 1xEV-DV kanal radio dan kanal radio yang lain yang dioperasikan dalam kaitannya dengan spesifikasi keluarga CDMA 2000.	Semua tipe <i>handoff</i> dimungkinkan antara IS-95, IS-95A, IS-95B, dan cdma2000 <i>Release A</i> , <i>Release B</i> , dan 1xEV-DV untuk panggilan suara. Suara panggilan tidak dapat di <i>handoff</i> ke sistim 1xEV-DV.
<i>Multiple</i> , sesi paket data yang konkuren setiap pengguna	

BAB III SISTIM KEAMANAN 1xEV-DV

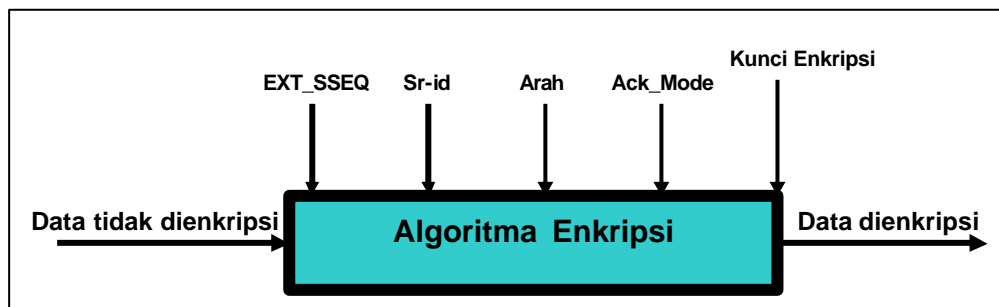
4.1. Enkripsi dan Otentifikasi dalam sistim 1xEV-DV

Sistim keamanan yang ada pada sistim 1xEV-DV yakni enkripsi dan otentifikasi sebagaimana pada CDMA 2000 pada umumnya. Berikut ini penjelasan tentang enkripsi dan otentifikasi.

4.1.1. Enkripsi

Teknik enkripsi yang digunakan dalam sistim 1xEV-DV sama dengan yang digunakan pada CDMA2000. *Mobile station* mengindikasikan ke *base station*, beberapa variasi algoritma enkripsi yang mendukungnya. *Base station* mempunyai keleluasaan untuk memutar *on/off* enkripsi sinyal data atau informasi data pengguna. *Mobile station* juga dapat mengusulkan untuk memutar enkripsi menjadi *on/off*. Pesan-pesan tidak dienkripsi jika otentifikasi tidak ditampilkan untuk pesan khusus. Selain itu juga, pesan-pesan yang pendek dikirimkan tanpa dienkripsi. Pesan-pesan yang membawa kapasitas *field* enkripsi cukup bervariasi berdasarkan nilai P_REV dari *mobile station*. Algoritma enkripsi yang digunakan 1xEV-DV adalah *Rijndael Encryption Algorithm*.

Algoritma enkripsi Rijndael merupakan algoritma yang aman dan sangat cepat. Algoritma enkripsi Rijndael (pengucapannya “Rhine-doll”) memungkinkan hanya ukuran kunci 128, 192 and 256-bit. 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. Kombinasi data ini kemudian dienkripsi menggunakan algoritma yang dijelaskan diatas.



Gambar 3. Enkripsi dalam 1xEV-DV

Tabel 3. Field Enkripsi

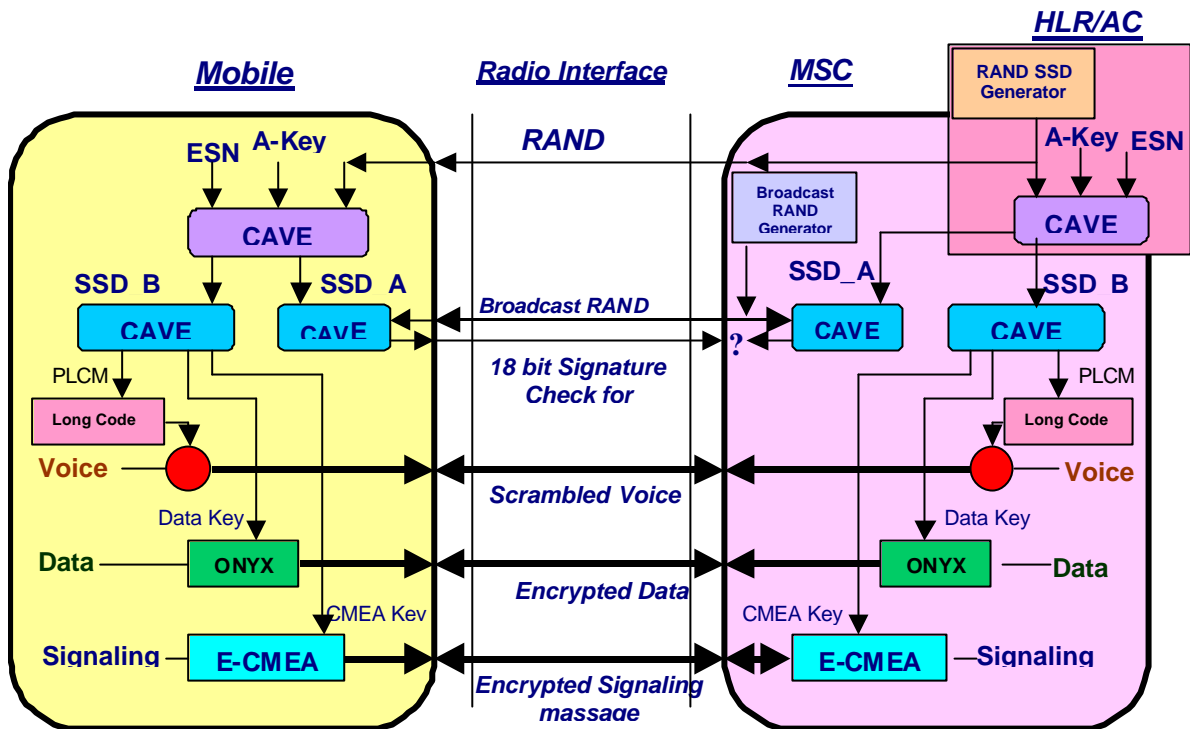
Field	Penjelasan
<i>EXT_SSEQ</i>	32 bit urutan jumlah enkripsi keamanan untuk enkripsi/dekripsi
<i>Sr_id</i>	<i>Identifier</i> Layanan Referensi untuk pilihan layanan cepat yang terkait
Arah	Arah data yang dienkripsi/dekripsi. Hal itu di set dengan "0" jika data diterima/dikirim pada kanal pengiriman, selain itu di set "1"
Kunci enkripsi	Kunci sesion untuk enkripsi. Hal ini merupakan hasil sukses perjanjian kunci Sesion antara mobile station dan base station
<i>Ack_Mode</i>	Mode pengiriman pesan. Hal ini diatur dengan set "0" jika pesan terkirim menggunakan mode un-assured, dan yang lainnya di set "1"

4.1.2. Otentifikasi (Authentication)

Otentifikasi merupakan proses dimana informasi dipertukarkan antara *mobile station* dan *base station* untuk mengkonfirmasi identitas mobile station. Prosedur otentifikasi dibawa dari CDMA 2000. *Base station* memiliki *Secret Shared Data* (SSD) yang mana unik untuk setiap *mobile station*. Jika kedua-duanya yakni *base station* dan *mobile station* memiliki set SSD yang identik, prosedur otentifikasi diperkirakan dapat sukses. Prosedur otentifikasi signatur (*Auth_Signature*) digunakan untuk menampilkan otentifikasi untuk *mobile station* tertentu. Parameter input berikut ini merupakan syarat dalam prosedur ini yakni:

- RAND_CHALLENGE
- ESN
- AUTH_DATA
- SSD_AUTH
- SAVE_REGISTERS

Otentifikasi ditampilkan menggunakan prosedur *Unique Challenge Procedure*. Dalam prosedur ini, *base station* mengenerate 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 digenerate, 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 otentifikasi gagal, maka akses selanjutnya melalui *mobile station* ditolak dan prosedur *updating* SSD dapat dilakukan.



Gambar 4. Mekanisme Otentifikasi dan Enkripsi

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). 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 digenerated pada HLR/AC, juga menjalankan peran dalam prosedur *authentication*. A-Key diprogram dalam *mobile* dan disimpan dalam *Authentication Center* (AC) jaringan. Sebagai tambahan pada *authentication*, yakni bahwa A-Key digunakan untuk mengenerate sub-key untuk *privacy* suara dan *message encryption*.

CDMA menggunakan standarisasi algoritma CAVE (*Cellular Authentication dan Voice Encryption*) untuk mengenerate 128-bit *sub-key* yang disebut “*Shared Secret Data*” (SSD). A-Key, ESN dan jaringan-supplied *RANDSSD* merupakan input ke CAVE yang mengenerate SSD. SSD memiliki dua bagian: SSD_A (64 bit), untuk membuat *authentication signatures* dan SSD_B (64 bit), untuk mengenerate 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.

Jaringan CDMA, *mobile* menggunakan SSD_A dan broadcast RAND* sebagai input terhadap algoritma CAVE untuk mengenerate 18-bit *authentication signature* (AUTH_SIGNATURE), dan mengirimkan ke *base station*. Signature ini juga kemudian digunakan oleh *base station* untuk memverifikasi legitimasi *subscriber*. Baik prosedur *Global Challenge* (dimana semua *mobile* merupakan *challenged* dengan jumlah *random* yang sama) dan *Unique Challenge* (dimana specific RAND digunakan untuk setiap permintaan *mobile*) dapat diperoleh operator untuk *authentication*. Metode *Global Challenge* memungkinkan terjadi *authentication* dengan sangat cepat. Juga, baik *mobile* dan *track* jaringan *Call History Count* (6-bit counter). Hal ini memberikan jalan untuk mendeteksi terjadinya, sebagaimana operator mendapat *alerted* jika ada gangguan. A-Key dapat diprogram ulang, tapi *mobile* dan jaringan *Authentication Center* harus diupdate. A-Key kemungkinan dapat diprogram oleh salah satu dari vendor berikut: a) Pabrik b). Dealer pada point penjualan c) Subscriber via telepon d) OTASP (over the air service provisioning). Transaksi OTASP memanfaatkan 512-bit perjanjian algoritma 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.

4.1.3. Voice, Signaling, and Data Privacy

Mobile menggunakan SSD_B dan algoritma CAVE untuk mengenerate *Private Long Code Mask* (diturunkan dari nilai intermediate yang disebut *Voice Privacy Mask*, yang mana menggunakan sistem legacy TDMA), *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*. Modifikasi *Long code* ini digunakan untuk penyadapan, yang mana menambahkan extra level privacy melalui CDMA interface udara. *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 kanal CDMA.

BAB IV PENUTUP

Perkembangan sistem komunikasi jaringan cdma2000 melalui 1x dengan nama CDMA2000 1xEV dengan dua tahap pengembangan yakni 1xEV-DO dan ²⁾ 1xEV-DV. Sistem 1xEV-DV adalah salah satu sistem jaringan komunikasi yang berbasis CDMA pada 3G dengan *interface* udara. Sistem 1xEV-DV merupakan fase kedua dari perkembangan CDMA 2000 yang menawarkan kompatibilitas yang lengkap sebagaimana dimiliki CDMA 2000. Sistem 1xEV-DV juga kompatibel dengan standar jaringan inti dari ANSI-41. CDMA 1x EV-DV yang merupakan mengimplementasikan sistem keamanan yakni enkripsi dan otentifikasi. Pada teknik enkripsi digunakan algoritma Rijndael (*Rijndael Encryption Algorithm*) yang aman dan sangat cepat dan hanya memungkinkan penggunaan ukuran kunci 128, 192 and 256-bit. Sedangkan pada otentifikasi menggunakan prosedur *Unique Challenge Procedure* dimana *base station* mengenerate 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".

Daftar Pustaka

- [1] Anonim, 2004. *EDGE, Telkomsel Pelopori Layanan 3G Indonesia*, Jakarta <http://www.edge.org> diakses tanggal 15 Juli 2004
- [2] Anonim, 2004. *CDMA2000*. <http://www.ericsson.com/cdmasystems/3gcdma2000.shtml> diakses tanggal 15 Juli 2004
- [3] Anonim, 2004. *cdmaOne: The Family of IS-95 CDMA Technologies*. <http://www.cdg.org/technology/2g.asp> diakses tanggal 15 Juli 2004
- [4] Anonim, 2004. *UMTS*. <http://www.umts-forum.org/servlet/dycon> diakses tanggal 15 Juli 2004
- [5] Anonim, 2000, *3G TR 33.900 V1.2.0 (2000-01)*, Valbonne-FRENCH
- [6] Anonim, 2001. *3GPP TS 33.120 V4.0.0 (2001-03)*, Valbonne-FRENCH
- [7] Anonim, 2001. *3GPP TS 33.105 V4.1.0 (2001-06)*, Valbonne-FRENCH
- [8] Dung Chang, 2002. *Security Along the Path Through GPRS Towards 3G Mobile Telephone Network Data*. Services Version 1.3. <http://www.sans.ac.usa> diakses tanggal 10 Oktober 2004
- [9] Tahar Ktari, David Mayor, 2004. *Security in GSM, GPRS AND 3GPP*. <http://www.3gpp.org> diakses tanggal 10 Oktober 2004
- [10] Anonim, 2002. *CDMA Evolution: cdma2000 1xEV-DV*. NOKIA. <http://www.3gpp.org> diakses tanggal 10 Oktober 2004
- [11] Sandeep Agrawal, Ira Acharya, Suhel Goel, 2003. *Inside 3G Wireless Systems: The 1xEV-DV Technology*, <http://www.3gpp.org> diakses tanggal 16 Oktober 2004
- [12] R. Thomas Derryberry, 2002. *CDMA2000 1x Evolved Data and Voice (1xEV-DV)*. Nokia Research Center, <http://www.3gpp.org> diakses tanggal 16 Oktober 2004
- [13] Bell Mobility, 2001. *HSDPA and 1xEV-DV, Harmonization Opportunities*. 3GPP/3GPP2 Joint Meeting on Harmonization of High Speed Data Services, <http://www.3gpp.org>. diakses tanggal 16 Oktober 2004
- [14] S. Agrawal, I. Acharya and S. Goel, *Inside 3G Wireless Systems: The 1xEV-DV Technology*, <http://www.3gpp.org>. diakses tanggal 16 Oktober 2004
- [15] Enrico Zanoio and Steve Urvik, *CDMA Network Technologies: A Decade of Advances and Challenges*, Tektronix, Inc. <http://www.3gpp.org>. diakses tanggal 16 Oktober 2004
- [16] Shawn A. Covell, 2003. *CDMA as a Broadband Access Technology*. QUALCOMM Southeast Asia . <http://www.3gpp.org>. diakses tanggal 16 Oktober 2004
- [17] Christopher Wingert, Mullaguru Naidu 2002, CDMA 1x RTT SECURITY, OVERVIEW, <http://www.3gpp.org>. diakses tanggal 16 Oktober 2004