KAJIAN SISTEM KEAMANAN JARINGAN CDMA

Sulistyo Unggul Wicaksono– NIM : 13503058

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail: if13058@students.if.itb.ac.id

Abstrak

Berdasarkan metode multiplexing-nya, teknik transmisi digital untuk sinyal radio dapat dibedakan menjadi tiga: CDMA (*Code-Division Multiple Access*), TDMA (*Time-Division Multiple Access*), dan FDMA (*Frequency-Division Multiple Access*). Ketiganya memiliki mekanisme pengamanan masing-masing. Makalah ini akan mengkaji sistem pengamanan pada jaringan CDMA, terutama CDMA2000 dan WCDMA. Pengkajian mencakup mekanisme dan algoritma-algoritma enkripsi yang digunakan dalam pengamanan komunikasi menggunakan jaringan CDMA pada aspek-aspek utama pengamanan jaringan *mobile* yaitu otentifikasi dan enkripsi (*Cellular Authentication and Voice Encryption*), proteksi data (ORYX), dan proteksi sinyal (*Cellular Message Encryption Algorithm*).

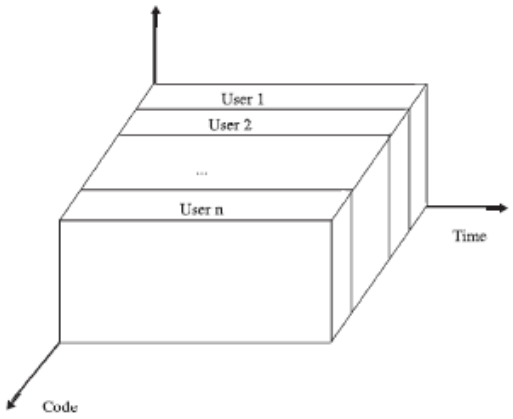
***Kata kunci**: Algoritma, Jaringan, Enkripsi, Otentifikasi, Proteksi Data dan Sinyal, CDMA, CDMA2000, WCDMA.*

1. 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. 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.

CDMA (*Code-Division Multiple Access*) adalah teknolgi selular digital yang menggunakan teknik spektrum tersebar. Pada awalnya, CDMA adalah teknologi militer yang digunakan di Perang Dunia II oleh Persekutuan Inggris sehingga menyulitkan Jerman untuk mengacaukan transmisi. Teknologi ini memungkinkan penyediaan kapasitas komunikasi data dan suara yang lebih baik dari teknologi mobile komersial lainnya. CDMA juga merupakan *platform* yang umum digunakan sebagai dasar pengembangan teknologi 3G.



Gambar 1. Code Division Multiple Access

Sejalan dengan prospeknya sebagai teknologi yang dapat memudahkan kehidupan manusia, CDMA juga harus dilengkapi dengan mekanisme pengamanan yang memadai. Ada tiga aspek penting dalam pengamanan jaringan komunikasi mobile: otentifikasi, proteksi data, dan anonimitas. Protokol pengamanan pada tiap

aspek tersebut penting untuk mengidentifikasi tingkat keamananan dari suatu jarinngan komunikasi mobile. Oleh sebab itu, makalah ini akan mengeksplorasi protokol-protokol pengamanan pada CDMA dan, lebih lanjut lagi, prospek CDMA dalam industri komunikasi mobile di dunia.

1.2. Roadmap Teknologi Komunikasi *Wireless*

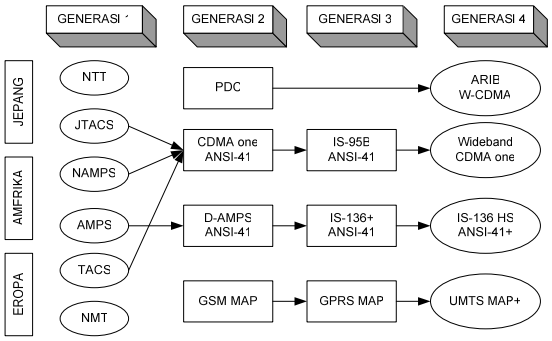
Kebutuhan akses informasi yang cepat akan terus berkembang. Hal tersebut dipengaruhi dengan adanya kebutuhan fleksibilitas dan produktifitas yang lebih tinggi dan kebutuhan mengurangi "*dead*" time. Kebutuhan-kebutuhan tersebut setidaknya akan terpenuhi dengan munculnya sistem komunikasi generasi ke-3. Hal ini dapat kita lihat karena dengan persyaratan-persyaratan yang harus dipenuhi untuk memasuki ke generasi tersebut.

Persyaratan yang dimaksud dapat diterangkan seperti di bawah ini :

- Layanan-layanan komunikasi dengan *data rate* yang tinggi dan transmisi data asimetrik
- Mendukung untuk *service* baik *packet* maupun *circuit switched*, seperti Internet (IP) trafik dan *video conference*
- Mekanisme *charging* yang baru, *data volume vs time*
- Kapasitas jaringan yang lebih besar dengan efisiensi spektrum
- Mendukung untuk koneksi yang besar dan simultan, contoh user dapat menelusuri Internet dan menerima fax atau panggilan telpon
- Mempunyai kapabilitas *interworking* dengan sistem eksisting
- Portabilitas layanan secara global

Sebelum menuju ke generasi di atas maka telah ada generasi sebelumnya yaitu generasi ke-1 dan generasi ke-2. Generasi ke-1 ditandai dengan teknologi analog sedangkan teknologi ke-2 yang ditandai dengan teknologi digital dengan kecepatan rendah.

Perkembangan menuju sistem komunikasi wireless generasi ke-3 (UMTS/IMT-2000) dapat diterangkan seperti gambar di bawah ini :



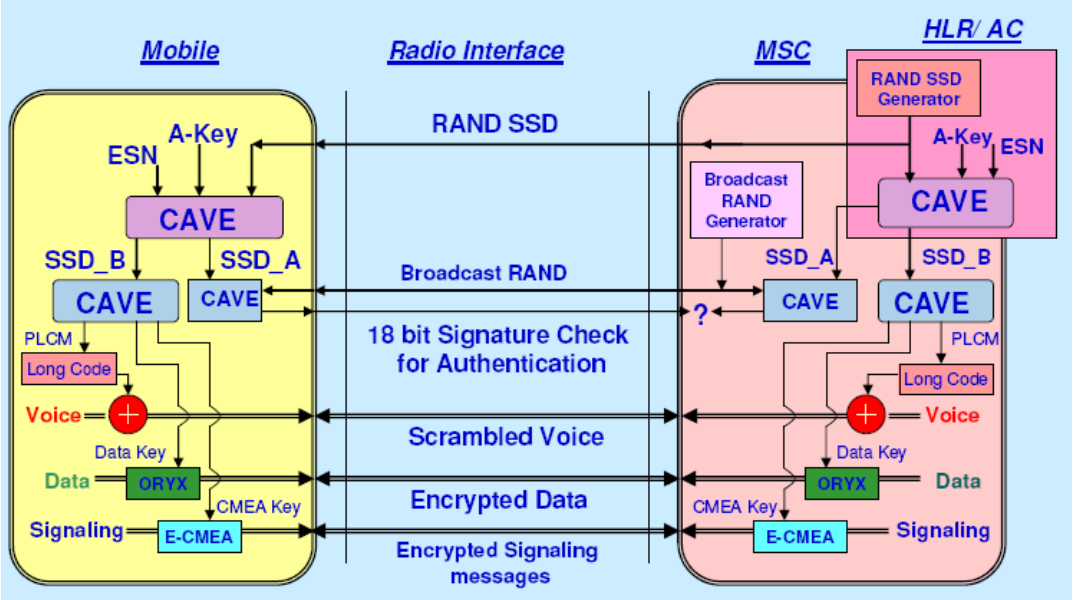
Gambar 2. Perkembangan sistem komunikasi *wireless*

Di Eropa ETSI bekerja untuk UMTS yang menjadi International Telecommunication Unit (IMT-2000). W-CDMA adalah salah satu kandidat utama untuk standar UMTS atau IMT-2000.

2. Sistem Keamanan Jaringan CDMA

Pada teknologi CDMA sistem keamanan yang diimplementasikan adalah enkripsi, otentifikasi, dan proteksi data dan sinyal. 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* meng-*generate* nilai 24-bit value dan mentransmisikannya ke *mobile station* di *Authentication Challenge Message*.



Gambar 3. Otentikasi dan Enkripsi di CDMA

Untuk lebih jelasnya, mekanisme otentifikasi dan enkripsi dapat dilihat pada Gambar 3.

Proteksi Data dan Sinyal CDMA

Teknologi CDMA 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).

CMEA pada CDMA digunakan untuk memproteksi sinyal. CMEA adalah blok cipher dengan kunci 64 bit. Ukuran bloknya dapat bervariasi. CMEA terdiri dari tiga layer. Layer pertama melakukan satu *non-linear pass* pada blok, yang mengakibatkan perputaran dari kiri ke kanan. Layer kedua adalah operasi linear tanpa kunci yang dilakukan untuk merubah propagasi ke arah sebaliknya. Operasi ini dapat dilakukan dengan meng-XOR-kan separuh blok bagian kanan ke separuh bagian kiri. Pada layer ketiga dilakukan *non-linear pass* terakhir pada blok dari kiri ke kanan, yang merupakan invers dari operasi pada layer pertama.

Sifat non-linear dari layer pertama dan ketiga didapatkan dari T box yang menghitung outputnya (8-bit) dengan cara:

$$T(x) = C(((C(((C(((C((x \oplus K_0) + K_1) + x) \oplus K_2) + K_3) + x) \oplus K_4) + K_5)+x) \oplus K_6) + K_7) + x$$

dengan x dan $K_{0...7}$ diketahui. Dalam persamaan ini C diperoleh dari CaveTable, dengan seluruh persamaan dihitung dengan aritmatika 8-bit

hi \ lo	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f
0.	d9	23	5f	e6	ca	68	97	b0	7b	f2	0c	34	11	a5	8d	4e
1.	0a	46	77	8d	10	9f	5e	62	f1	34	ec	a5	c9	b3	d8	2b
2.	59	47	e3	d2	ff	ae	64	ca	15	8b	7d	38	21	bc	96	00
3.	49	56	23	15	97	e4	cb	6f	f2	70	3c	88	ba	d1	0d	ae
4.	e2	38	ba	44	9f	83	5d	1c	de	ab	c7	65	f1	76	09	20
5.	86	bd	0a	f1	3c	a7	29	93	cb	45	5f	e8	10	74	62	de
6.	b8	77	80	d1	12	26	ac	6d	e9	cf	f3	54	3a	0b	95	4e
7.	b1	30	a4	96	f8	57	49	8e	05	1f	62	7c	c3	2b	da	ed
8.	bb	86	0d	7a	97	13	6c	4e	51	30	e5	f2	2f	d8	c4	a9
9.	91	76	f0	17	43	38	29	84	a2	db	ef	65	5e	ca	0d	bc
a.	e7	fa	d8	81	6f	00	14	42	25	7c	5d	c9	9e	b6	33	ab
b.	5a	6f	9b	d9	fe	71	44	c5	37	a2	88	2d	00	b6	13	ec
c.	4e	96	a8	5a	b5	d7	c3	8d	3f	f2	ec	04	60	71	1b	29
d.	04	79	e3	c7	1b	66	81	4a	25	9d	dc	5f	3e	b0	f8	a2
e.	91	34	f6	5c	67	89	73	05	22	aa	cb	ee	bf	18	d0	4d
f.	f5	36	ae	01	2f	94	c3	49	8b	bd	58	12	e0	77	6c	da

Gambar 4. CaveTable

Spesifikasi CMEA dapat diperlihatkan dengan algoritma di bawah ini. Algoritma ini mengenkripsi sebuah pesan n-byte $P_{0,...,n-1}$ ke cipherteks $C_{0,...,n-1}$ dengan key $K_{0...7}$ dengan cara:

$y_0 \leftarrow 0$
for $i \leftarrow 0, \ldots, n-1$
$\quad P'_i \leftarrow P_i + T(y_i \oplus i)$
$\quad y_{i+1} \leftarrow y_i + P'_i$

for $i \leftarrow 0, \ldots, \lfloor \frac{n}{2} \rfloor - 1$
$\quad P''_i \leftarrow P'_i \oplus (P'_{n-1-i} \vee 1)$

$z_0 \leftarrow 0$
for $i \leftarrow 0, \ldots, n-1$
$\quad z_{i+1} \leftarrow z_i + P''_i$
$\quad C_i \leftarrow P''_i - T(z_i \oplus i)$

Setiap operasi adalah aritmatika byte + dan – adalah pertambahan dan pengurangan modulo 256, dan fungsi T diperoleh dari persamaan sebelumnya.

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.

ORYX adalah cipher aliran sederhana yang berbasis *linear feedback shift registers* (LFSRs) yang digunakan sistem seluler digital untuk memproteksi data seluler. ORYX cipher digunakan sebagai generator *keystream*. Keluaran dari generator adalah *bytes sequence* yang random. Proses enkripsi dilakukan dengan meng-XOR–kan *keystream bytes* dengan *data bytes*. Sebaliknya, dekripsi dilakukan dengan meng-XOR-kan *keystream bytes* dengan ciphertext.

Dari situ, diketahui bahwa pasangan plaintext-ciphertext dapat digunakan untuk memulihkan segmen-segmen keystream.

ORYX cipher mempunyai empat komponen: tiga LFSRs 32-bit yang dinotasikan $LFSR_A$, $LFSR_B$ dan $LFSR_K$, dan sebuah S-box yang berisi permutasi L yang mencakup nilai-nilai integer dari 0 sampai 255, termasuk 0 dan 255.

Fungsi feedback untuk $LFSR_K$ adalah:

$x^{32} + x^{28} + x^{19} + x^{18} + x^{16} + x^{14} + x^{11} + x^{10} + x^9 + x^6 + x^5 + x + 1.$

Fungsi feedback untuk $LFSR_A$ adalah:

$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1.$

dan

$x^{32} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{17} + x^{13} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^2 + x + 1.$

Fungsi feedback untuk $LFSR_B$ adalah:

$x^{32} + x^{31} + x^{21} + x^{20} + x^{16} + x^{15} + x^6 + x^3 + x + 1.$

Permutasi L nilainya tetap dalam satu pemanggilan algoritma, dibentuk dari algoritma yang diketahui, diinisialisasi dengan sebuah nilai yang ditransmisikan dalam persiapan pemanggilan algoritma. Setiap *keystream bytes* dibangkitkan dengan langkah-langkah sebagai berikut:

1. $LFSR_K$ dipanggil satu kali.
2. $LFSR_A$ dipanggil satu kali, dengan satu dari dua polinomial feedback yang berbeda dihitung berdasarkan nilai tingkatan $LFSR_K$.
3. $LFSR_B$ dipanggil satu kali atau dua kali, tergantung pada nilai dari tingkatan lain dari $LFSR_K$.
4. *High bytes* dari $LFSR_K$, $LFSR_A$, dan $LFSR_B$ dikombinasikan untuk membentuk *byte keystream* menggunakan fungsi berikut:

Keystream = $\{High8_K + L[High8_A] + L[High8_B]\}$ mod 256

Selanjutnya, akan dikaji lebih spesifik mengenai keamanan varian teknologi CDMA. Varian teknologi CDMA yang akan dibahas disini meliputi CDMA2000 dan WCDMA.

2.1. CDMA2000

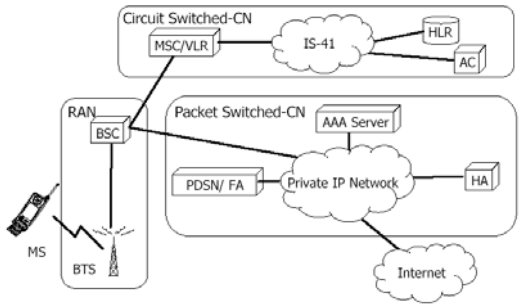
2.1.1. Arsitektur Jaringan CDMA2000

Jaringan CDMA2000 mempunyai komponen-komponen sebagai berikut :

- *Mobile Station* (MS)
  Mempunyai fungsi utama untuk membentuk, memelihara dan membubarkan hubungan (voice dan data) dengan jaringan. MS membentuk hubungan dengan meminta kanal radio dari RN. Setelah hubungan terbentuk MS bertanggung jawab untuk menjaga kanal radio tersebut dan melakukan buffer paket jika kanal radio sedang tidak tersedia. MS biasanya mendukung enkripsi dan protokol seperti Mobile IP dan Simple IP.

- *Radio Network* (RN)
  Terdiri dari dua komponen yaitu *Packet Control Function* (PCF) dan *Radio Resources Control* (RRC).
  Fungsi utama PCF adalah untuk membentuk, memelihara dan membubarkan hubungan dengan PDSN. PCF berkomunikasi dengan RRC untuk meminta dan mengatur kanal radio untuk menyampaikan paket dari dan ke MS. PCF juga bertanggung jawab mengumpulkan informasi akunting dan meneruskannya ke PDSN. RRC mendukung otentikasi dan otorisasi MS untuk mendapatkan akses radio. RRC juga mendukung enkripsi air interface bagi MS.

- *Packet Data Serving Node* (PDSN)
  PDSN melakukan bermacam-macam fungsi. Yang utama adalah melakukan routing paket ke jaringan IP atau ke HA. Dia memberikan alamat IP dinamik dan menjaga sesi *Point-To-Point Protocol* (PPP) ke MS. Dia memulai otentikasi, otorisasi dan akunting ke AAA untuk sesi paket data. Sebagai balasannya PDSN menerima parameter-parameter profil pelanggan yang berisi jenis-jenis layanan dan keamanan.



Gambar 5. Arsitektur jaringan CDMA2000

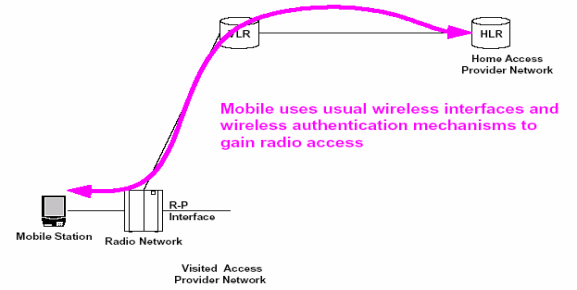
- *Home Agent* (HA)
  HA berperan dalam implementasi protokol Mobile IP dengan meneruskan paket-paket ke FA dan sebaliknya. HA menyediakan keamanan dengan melakukan otentikasi MS melalui pendaftaran Mobile IP. HA juga menjaga hubungan dengan AAA untuk menerima informasi tentang pelanggan.

- *Authentication, Authorization and Accounting* (AAA)
  AAA mempunyai peran yang berbeda-beda tergantung pada tipe jaringan dimana dia terhubung. Jika AAA server terhubung ke service provider network, fungsi utamanya adalah melewatkan permintaan otentikasi dari PDSN ke Home IP network, dan mengotorisasi respon dari home IP network ke PDSN. AAA juga menyimpan informasi akunting dari MS dan menyediakan profil pelanggan dan informasi QoS bagi PDSN.
  Jika AAA server terhubung ke home IP network, dia melakukan otentikasi dan otorisasi bagi MS berdasarkan permintaan dari AAA lokal.
  Jika AAA terhubung ke broker network, dia meneruskan permintaan dan respon antara service provider network dan home IP network yang tidak mempunyai hubungan bilateral.

2.1.2 AAA pada CDMA2000

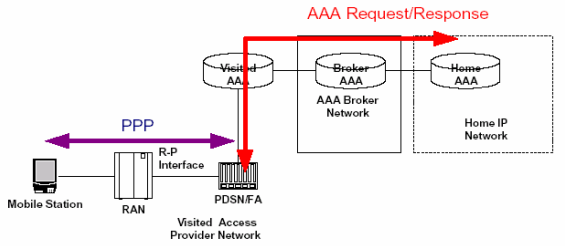
AAA merupakan kepanjangan dari Authentication, Authorization, dan Accounting. Otentikasi adalah kegiatan seseorang memverifikasi bahwa sesuatu itu valid atau sah. Otorisasi adalah penentuan apakah sesuatu (user atau peralatan) itu mempunyai ijin untuk mengakses layanan. Dan akunting mempunyai arti melakukan tracking tentang siapa, apa, kapan dan dimana permintaan berasal dan kemana respon akan dikirimkan. AAA sangat penting

dalam jaringan nirkabel karena adanya roaming dan identitas user yang harus selalu dijaga, dan sistem harus terus memantau aktifitas user tersebut.



Gambar 6. Otentifikasi dan Otorisasi RN

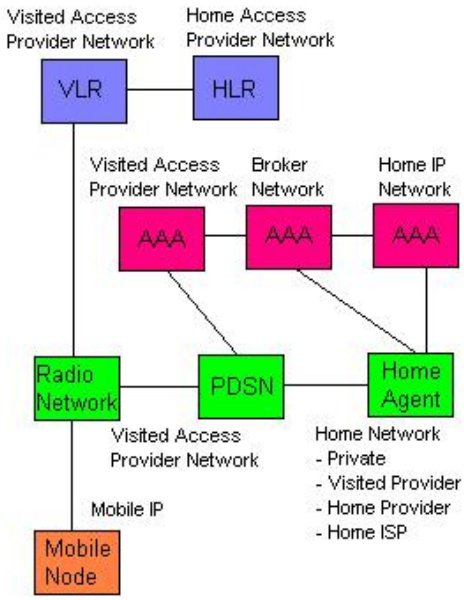
Otentikasi MS dilakukan oleh radio network dan IP network. Pada otentikasi IP network, MS menggunakan *Challenge Handshake Authentication Protocol* (CHAP) untuk layanan tradisional PPP, dan menggunakan *Foreign Agent Challenge* (FAC) pada layanan Mobile IP. Kedua otentikasi tersebut tetap menggunakan infrastruktur AAA yang sama.



Gambar 7. Otentifikasi IP network

Jaringan CDMA2000 dapat dilihat dalam tiga entitas primer yaitu :

- RN yang terdiri dari *Base Station* (BS) dan PCF
- Circuit switched core network yaitu MSC, *Visitor Location Register* (VLR) dan *Home Location Register* (HLR)
- Packet data core network yaitu PDSN, HA dan AAA



Gambar 8. AAA dalam jaringan CDMA2000

Server AAA berinteraksi dengan *Foreign Agent* (FA) dan server AAA lainnya untuk melakukan fungsi-fungsi keamanan bagi mobile client. Server AAA bertanggung jawab pada mekanisme untuk mendukung keamanan antara MS dan agent.

AAA dalam CDMA2000 harus memenuhi beberapa persyaratan. Persyaratan layanan secara umum antara lain :

- Menyediakan layanan selama pelanggan berada dalam sistem jaringan
- Mendukung layanan PPP (Simple IP) dan Mobile IP :
- Mendukung dinamic dan static home address assignment untuk Mobile IP
- Mendukung HA dalam jaringan dimana MS berada
- Mendukung IP Security pada Mobile IP tunnel antara FA dan HA
- Menyediakan layanan AAA
- Menyediakan pemisahan antara airlink resource dan data resource dalam layanan AAA
- Melakukan otentikasi dan otorisasi MS berdasarkan *International Mobile Station Identity* (IMSI) dan *Network Access Identifier* (NAI)
- Mendukung layanan AAA broker
- Mengijinkan distribusi informasi security key Mobile IP untuk mendukung home agent assignment, fast handoff, dan fast HA – FA authentication assignment

- Menyediakan QoS pada high level architecture

Dalam hubungan dengan AAA, elemen-elemen jaringan dalam gambar 4 mempunyai fungsi sebagai berikut :

PDSN:
- Bertindak sebagai FA
- Membentuk, menjaga, dan memutuskan hubungan ke MS
- Memulai otentikasi, otorisasi dan akunting bagi MS
- Mengamankan saluran ke HA dengan menggunakan IP Security
- Menerima parameter-parameter layanan dari AAA untuk MS
- Mengumpulkan data-data akunting untuk dikirimkan ke AAA
- Melakukan routing paket ke jaringan paket data eksternal
- Melakukan mapping home address dan HA address untuk identifier yang digunakan untuk komunikasi dengan RN

AAA server:
- Berinteraksi dengan FA dan server AAA lainnya untuk otentikasi, otorisasi dan melakukan proses akunting bagi MS
- Menyediakan mekanisme untuk mendukung keamanan antara PDSN/FA dan HA, antara MS dan PDSN/FA
- Mengidentifikasi HA secara dinamik dan menyediakan keamanan bersama antara MS dan HA
- Menyediakan informasi QoS bagi PDSN
- Menentukan dynamic home address

RN:
- Melakukan validasi MS untuk mengakses layanan
- Mengatur koneksi layer fisik ke MS
- Menjaga keadaan reachability bagi layanan paket antara RN dan MS
- Melakukan buffer paket yang datang dari PDSN jika radio resource tidak tersedia
- Me-relay paket-paket antara MS dan PDSN

Location Register (VLR/HLR) :
- Menyimpan informasi otentikasi dan otorisasi bagi RN

HA:
- Menjaga registrasi user dan meneruskan paket ke PDSN
- Membentuk IP secure tunnel ke PDSN/FA
- Mendukung dynamic HA assignment
- Mendukung dynamic home address
- Mendukung reverse tunneling

MS:
- Mendukung PPP
- Dapat bertindak sebagai Mobile IP Node dan mendukung FAC dan NAI
- Berinteraksi dengan RN untuk mendapatkan radio resource dari jaringan
- Menjaga informasi mengenai status radio resource (misalnya aktif, standby, tidak aktif)
- Melakukan buffer paket jika radio resource tidak tersedia untuk mendukung flow ke jaringan

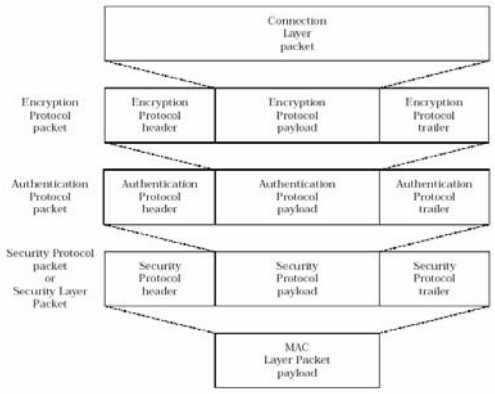
Persyaratan inti yang harus ada pada AAA server adalah :
- Melakukan otentikasi dan otorisasi NAI pelanggan pada lingkungan roaming. NAI diperoleh melalui CHAP (untuk layanan tradisional PPP) atau FAC (untuk layanan Mobile IP). Terdapat *shared secret* antara MS dengan HAAA-nya.
- Membawa atribut-atribut data dari home network ke serving network.
- Enkrip pesan AAA antara home, serving network atau broker.
- Mendukung mekanisme tansport AAA yang reliable
- Mekanisme transport ini akan dapat memberi tanda pada suatu aplikasi AAA bahwa pesan telah dikirimkan ke aplikasi AAA berikutnya atau bahwa telah terjadi time-out.
- Pengiriman kembali (re-transmision) dikontrol oleh mekanisme transport AAA, dan bukan oleh protokol lapisan bawah seperti TCP
- Jika pesan AAA akan diteruskan, atau pilihan pesan tidak sesuai dengan protokol AAA, mekanisme transport tetap akan memberi tahu bahwa node telah menerima pesan AAA.
- *Acknowledgement* diijinkan dalam pesan-pesan AAA.
- Fitur dalam mekanisme transport harus mempunyai kemampuan untuk mendeteksi *silent failure* dan mengatasi kegagalan tersebut secara proaktif.

- Membawa sertifikat digital dalam pesan AAA untuk meminimalkan jumlah round trip dalam transaksi AAA.
- Mendukung proxy dan non-proxy broker. AAA broker harus mempunyai kemampuan untuk memodifikasi bagian-bagian tertentu dalam pesan AAA agar dapat beroperasi dalam lingkungan proxy atau non-proxy.
- Menyediakan *message integrity* dan *identity authentication* pada tiap node AAA.
- Mendukung *replay protection* dan kemampuan *non-repudiation* pada semua pesan otorisasi dan akunting.
- Mendukung accounting melalui perjanjian bilateral dan melalui server AAA broker.

Menyediakan keamanan antara server-server AAA, dan antara server AAA dengan PDSN atau HA melalui IP Security.

2.1.3 Keamanan CDMA2000

Protokol keamanan pada CDMA merupakan yang terbaik dibandingkan pada metode akses yang lain (TDMA/FDMA). Hal ini dikarenakan, pada CDMA tiap user menggunakan *unique code* yang berbeda-beda sehingga sulit untuk disadap. Unique code disini adalah urutan 42-bit *Pseudo-random Noise* (PN) yang digunakan untuk mengacak (*scramble*) voice dan data yang dikirim. Pada forward link (network to mobile) data diacak pada rate 19.2 Ksps (symbols per second), dan pada reverse link data diacak pada rate 1.2288 Mcps (chips per second).
Gambar di bawah memperlihatkan hubungan antara paket pada Connection Layer, paket pada Encryption Layer, paket pada Authentication Layer, paket pada Security Layer dan paket pada MAC Layer.



Gambar 9. Security layer encapsulation

Ketika paket dari Connection Layer yang akan dienkripsi atau diotentikasi dikirimkan ke Security layer, maka protokol-protokol dalam Security layer akan melakukan langkah-langkah berikut :

- Protokol Security layer membangkitkan cryptosync bagi kanal tujuan paket tersebut.
- Paket Connection Layer dan nilai dari cryptosync dikirimkan ke Encryption Protocol.
- Jika paket Connection Layer akan dienkripsi, Encryption Protocol menggunakan Cryptosync, encryption key dan parameter lain untuk mengenkripsi paket Connection Layer dan membentuk paket Encryption Protocol.
- Encryption Protocol mengirimkan paket Encryption Protocol dan Cryptosync ke Authentication Protocol.
- Jika paket Encryption Protocol akan diotentikasi, maka Authentication Protocol menggunakan Cryptosync, authentication key dan parameter lain untuk membentuk paket Authentication Protocol.
- Authentication Protocol mengirimkan paket Authentication Protocol dan Cryptosync ke Security Protocol.
- Security Protocol menggunakan Cryptosync untuk membentuk header dan trailer Security Protocol.
- Security Protocol mengirimkan paket Security Protocol ke MAC layer.

Sebaliknya jika Security layer menerima paket MAC layer yang terenkripsi, protokol-protokol dalam Security layer akan melakukan langkah-langkah berikut :

- Security Protocol membentuk cryptosync dengan menggunakan header dan trailer Security Protocol.
- Security Protocol membuang header dan trailer kemudian mengirimkan cryptosync dan paket Security Protocol ke Authentication Protocol.
- Jika paket Authentication Protocol terotentikasi, maka Authentication Protocol melakukan verifikasi authentication signature dengan menggunakan cryptosync, authentication key, payload Authentication Protocol, header dan trailer Authentication Protocol dan parameter lainnya. Jika authentication

signature sesuai (lolos), maka Authentication Protocol mengirimkan payload Authentication Protocol ke Encryption Protocol. Jika authentication signature tidak sesuai (tidak lolos) maka paket akan dibuang.

- Jika paket Authentication Protocol tidak terotentikasi maka payload Authentication Protocol akan langsung dikirim ke Encryption Protocol.
- Jika paket Encryption Protocol terenkripsi, maka Encryption Protocol menggunakan cryptosync dan encryption key untuk men-dekrip paket Encryption Protocol. Paket yang telah didekrip kemudian dikirimkan ke Connection layer.
- Jika paket Encryption Protocol tidak terenkripsi maka paket tersebut akan langsung dikirim ke Connection layer.
- Security layer menyediakan dua pasang informasi keamanan bagi Connection layer. Yang pertama mengindikasikan :
- Apakah konfigurasi Security layer mendukung enkripsi paket Security layer ataukah tidak.
- Apakah Security layer men-dekrip paket Security layer ataukah tidak.

Yang kedua mengindikasikan :

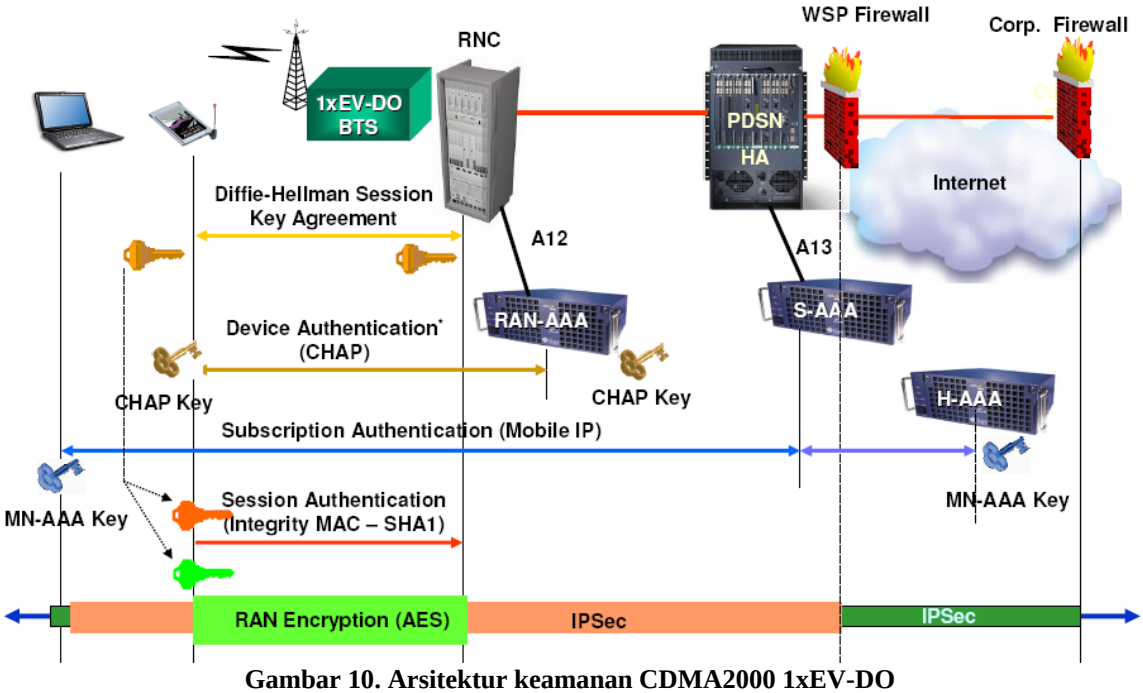
- Apakah konfigurasi Security layer mendukung enkripsi paket Security layer ataukah tidak.
- Apakah Security layer mengotentikasikan paket Security layer ataukah tidak.

Aplikasi atau protokol penerima dapat menggunakan informasi keamanan ini untuk menentukan apakah payload akan dibuang atau tidak.

Komponen-komponen keamanan pada CDMA2000 meliputi *key management, authentication procedure* dan enkripsi dan *privacy*. Sedangkan algoritma keamanan yang digunakan meliputi :

- CAVE : untuk otentikasi dan pembuatan kunci
- CMEA : untuk enkripsi control data
- ORYX : untuk enkripsi user data
- SS dengan LFSR mask : untuk enkripsi suara

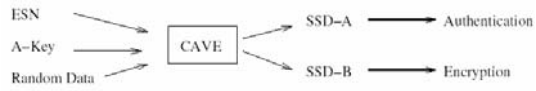
Sebagai contoh gambaran, arsitektur keamanan CDMA2000 1xEV-DO dapat dilihat pada Gambar 10 dibawah ini.



Gambar 10. Arsitektur keamanan CDMA2000 1xEV-DO

2.1.3.1. Manajemen kunci

Protokol keamanan jaringan CDMA2000 berbasis pada 128-bit *authentication key* (A-key) dan *Electronic Serial Number* (ESN) pada MS. A-key diprogram pada MS (RUIM) dan juga disimpan dalam *Authentication Center* (AC) di jaringan. A-key juga berfungsi dalam menghasilkan sub-key untuk *voice privacy* dan *message encryption*.
CDMA2000 menggunakan algoritma *Cellular Authentication and Voice Encryption* (CAVE) untuk menghasilkan 128-bit sub-key yang disebut *Shared Secret Data* (SSD). A-key, ESN dan RANDSSD yang dihasilkan oleh HLR/AC, merupakan input bagi CAVE sehingga menghasilkan SSD. SSD terdiri dari dua bagian yaitu SSD_A (64 bit) untuk membuat *authentication signature* dan SSD_B (64 bit) untuk membangkitkan kunci untuk enkripsi voice dan *signaling messages*. SSD dapat digunakan bersama dengan VLR dan bertujuan untuk mengijinkan otentikasi lokal.



Gambar 11. Proses menghasilkan SSD

2.1.3.2. Otentifikasi

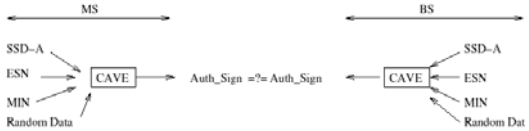
Otentikasi untuk akses jaringan CDMA2000 merupakan dua tahapan proses. Pertama adalah otentikasi MS oleh MSC/VLR. Otentikasi ini diperlukan untuk akses ke jaringan circuit-sitched (yang mendukung layanan voice) dan akses ke jaringan paket data. Tahap kedua adalah otentikasi ke jaringan paket data melalui PDSN dan AAA atau HA. Otentikasi ini memungkinkan MS untuk mengakses jaringan paket data.

Saat ini otentikasi PPP (menggunakan PAP atau CHAP) digunakan untuk otentikasi user yang mengakses layanan Simple IP. Jika user menggunakan Mobile IP, otentikasinya berdasarkan skema Challenge Response dengan algoritma SHA-1. Tetapi dalam semua kasus, PDSN mengandalkan infrastruktur AAA dengan RADIUS backend untuk otentikasi jaringan paket data.

Otentikasi pada CDMA2000 terdiri dari dua komponen yaitu :

- *Challenge-Response authentication*
  Menggunakan protokol *Authentication and Key Agreement* (AKA)
- *Message integrity checks*
  Menggunakan *Secure Hashing Algorithm – 1* (SHA-1) untuk hashing dan integrity

Dalam jaringan CDMA, MS menggunakan SSD_A dan broadcast RAND (yang dibangkitkan oleh MSC) sebagai input bagi algoritma CAVE untuk membangkitkan 18-bit *authentication signature* (AUTH_SIGNATURE) dan mengirimkannya ke base station. Signature ini kemudian digunakan oleh BS untuk memverifikasi bahwa subscriber tersebut sah.



Gambar 12. Proses otentifikasi secara umum

Otentikasi terjadi ketika MS berusaha mendaftar atau melakukan panggilan. Prosedur *Global Challenge* dan *Unique Challenge* tersedia bagi operator untuk keperluan otentikasi. Global Challenge merupakan prosedur dimana semua MS ditantang (*challenged*) dengan *random number* yang sama, sedangkan Unique Challenge merupakan prosedur dimana suatu RAND spesifik digunakan untuk tiap permintaan dari MS. Metode Global Challenge memungkinkan otentikasi dilakukan secara sangat cepat. MS dan jaringan bersama-sama melakukan tracking *Call History Count* (counter 6-bit) dan cara ini berguna untuk mendeteksi adanya kloning, sementara operator akan mendapat peringatan jika terjadi ketidakcocokan.

A-key dapat diprogram kembali (*re-programmable*) dan pemrograman tersebut dapat melalui salah satu cara berikut ini :

- Oleh pabrik
- Oleh dealer pada tempat-tempat penjualan
- Oleh pelanggan melalui telepon
- OTASP (*over the air service provisioning*)

Transaksi OTASP memanfaatkan algoritma *512-bit Diffie-Hellman key agreement*. A-key pada MS dapat diubah melalui OTASP sehingga memudahkan bagi pelanggan. Keamanan A-key ini merupakan komponen yang paling penting dalam sistem CDMA.

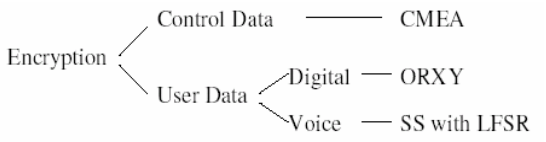
2.1.3.3. Enkripsi dan Proteksi Data

Privacy dalam sistem CDMA2000 dapat dibedakan menjadi dua yaitu :

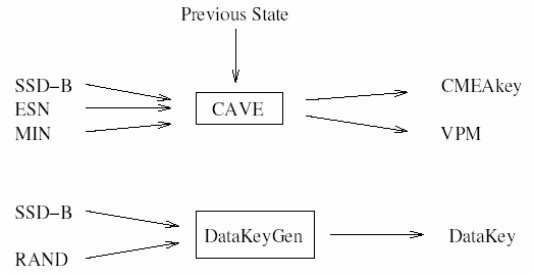
- *Identity privacy*
  Sistem CDMA menyediakan *Temporary Mobile Station Identifier* (TMSI) bagi MS selama MS melakukan komunikasi melalui transmisi udara.
- *User data privacy*
  Memanfaatkan kunci-kunci CMEA dan Data dengan algoritma ECMEA dan ORYX

MS menggunakan SSD_B dan algoritma CAVE untuk membangkitkan *Private Long Code Mask* (diturunkan dari *Voice Privacy Mask*), *Cellular Message Encryption Algorithm* (CMEA) key (64 bit) dan Data key (32 bit). Private Long Code Mask digunakan oleh MS dan jaringan untuk mengubah karakteristik long-code. Long code yang dimodifikasi ini digunakan untuk pengacakan suara, sehingga menambah level privacy pada interface udara CDMA. Private Long Code Mask tidak meng-enkrip informasi, tetapi hanya mengganti nilai sinyal encoding dengan nilai private yang hanya diketahui oleh MS dan jaringan. Karena itu sulit untuk menyadap percakapan tanpa mengetahui Private Long Code Mask.

Dalam sistem CDMA, MS dan jaringan menggunakan CMEA key dengan algoritma *Enhanced CMEA* (ECMEA) untuk enkripsi pesan-pesan pensinyalan (*control data*) yang dikirimkan melalui udara dan untuk dekripsi informasi yang diterima. Data key dan ORYX (algoritma untuk enkripsi user data digital) digunakan oleh MS dan jaringan untuk enkripsi dan dekripsi user data pada kanal-kanal CDMA.



Gambar 13. Enkripsi pada CDMA



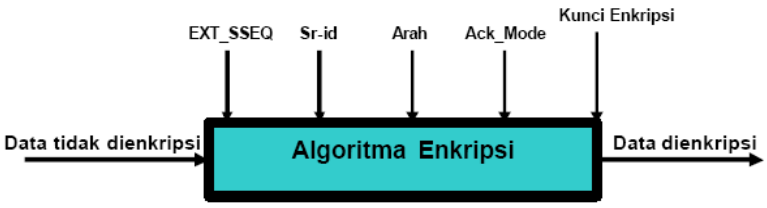
Gambar 14. Kunci yang digunakan untuk enkripsi

CDMA 2000 Berikut sistem pengamanan pada teknologi CDMA2000 1xEVDV.

Enkripsi CDMA2000 1xEVDV

Teknik enkripsi yang digunakan dalam sistem 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 dan 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 15. Enkripsi dalam 1xEV-DV

Field	Penjelasan
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"
Kinci enkripsi	Kunci sesion untuk enkripsi. Hal ini merupakan hasil sukse perjanjian kunci Sesion antara mobile station dan base station
Ack_Mode	Mode pengiriman pesan. Hal ini diatur dengan set "0" jika pesan terkirim menggunakan mo de un-assured, dan yang lainnya di set "1"

Tabel 1. Field Enkripsi

Otentifikasi CDMA2000 1xEVDV

Otentifikasi merupakan proses dimana informasi dipertukarkan antara mobile station dan base station untuk mengkonfirmasikan 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.

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.

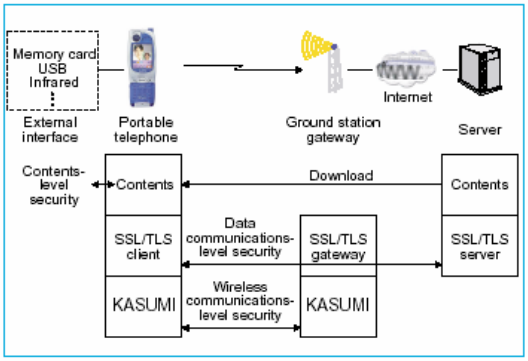
CDMA menggunakan standarisasi algoritma CAVE (Cellular Authentication dan Voice Encryption) untuk mengenerate 128-bit sub-key yang disebut “Shared Secret Data” (SSD). AKey, ESN dan jaringan-supplied RANDSSD merupakan input ke CAVE yang mengenerate SSD. SSD memiliki dua bagian: SSD_A (64 bit), untuk membuat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

2.1.4 Keamanan WCDMA

Teknologi keamanan yang diperlukan dalam sistem telepon mobile W-CDMA, termasuk fungsi keamanan pada level-komunikasi suara, fungsi keamanan pada level komunikasi data dan fungsi keamanan pada level isi (contents). Gambar dibawah menunjukkan teknologi keamanan yang diterapkan pada telepon mobile W-CDMA.



Gambar 16. Teknologi keamanan W-CDMA

2.1.4.1. Tingkat keamanan otentifikasi pada komunikasi nirkable

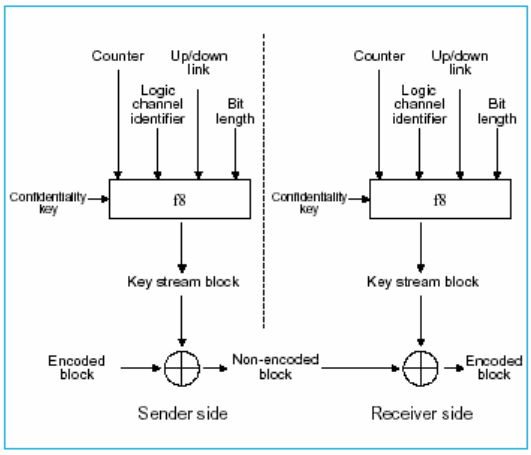
Ini adalah suatu teknologi untuk membuktikan keaslian pemakai yang mempunyai otoritas untuk menggunakan fasilitas komunikasi nirkabel, atau dengan kata lain, bahwa pemakai adalah pelanggan telah membayar jasa layanan komunikasi dan untuk mendeteksi perubahan data yang tidak sah. Ini juga dikenal sebagai otentifikasi (pengesahan) pesan (message). Fungsi F9 digunakan untuk menghasilkan kode otentifikasi (pengesahan) itu untuk ditambahkan kepada data dalam urutan pesanan ketika suatu panggilan diminta, sisi jaringan membuktikan keaslian telepon mobile berdasar pada informasi pelanggan yang ada dalam handset. Jika informasi pelanggan telah dikirim kepada sisi jaringan dalam mode plain-text, informasi ini masih memungkinkan untuk disadap orang lain dan dengan sukses memainkan peran (menyamar) sebagai pelanggan yang asli.

Otentifikasi (pengesahan) kemudian dilakukan oleh kedua sisi yang untuk melakukan

perhitungan menggunakan informasi pelanggan dan membandingkan hasilnya. Di dalam W-CDMA, ada fungsi f1 ke f5 yang menggambarkan proses itu dengan mana kalkulasi dilakukan. Algoritma di dalam fungsi ini tidak mengacu pada standardisasi, tetapi lebih ditentukan oleh para operator komunikasi nirkabel itu. Dalam proses kalkulasi untuk otentifikasi (pengesahan) telepon mobile dan jaringan saling berbagi kunci otentifikasi (pengesahan) itu dan mencegah perubahan data kunci secara tidak sah.

2.1.4.2. Otentifikasi (Pengesahan) Data

Dalam W-Cdma, fungsi f8 digunakan untuk menghasilkan satu rangkaian angka-angka secara acak, dan logika eksklusif OR (X-OR) melakukan penjumlahan untuk masing-masing bit data pemakai dan sinyal data untuk melakukan encoding (penyandian). Panjang bit untuk encoding/decoding, up/down link, counter, pengidentifikasi saluran yang logis, dan kunci untuk kerahasiaan data dimasukkan kedalam fungsi logika f8 untuk menghasilkan deretan angka-angka secara acak.



Gambar 17. Fungsi f8 untuk menjamin kerahasiaan data

2.1.4.3. Integritas Data

Ini mengacu pada teknologi yang mana kode otentifikasi (pengesahan) ditambahkan ke sinyal data di dalam komunikasi nirkabel dalam rangka mendeteksi perubahan data yang tidak sah. Ini juga dikenal adalah otentifikasi (pengesahan) pesan. Fungsi F9 digunakan untuk menghasilkan kode otentifikasi (pengesahan) itu untuk ditambahkan pada data dalam rangka melihat kemungkinan perubahan data yang tidak sah dan memastikan integritas data. Data, up/down link, counter, suatu nomor acak untuk masing-masing pemakai, dan kunci integritas dimasukkan ke dalam fungsi f9 untuk menghasilkan kode pengesahan pesan (message-authentication code). Penerima membandingkan kode pengesahan pesan yang dikirim oleh pengirim kepada kode pengesahan pesan yang dihasilkan oleh penerima, ini membuat kemungkin untuk konfirmasi, ketika kode itu cocok (match), yang menunjukkan tidak ada perubahan data secara tidak sah.

2.1.4.4. Algoritma Enkripsi KASUMI

Algoritma enkripsi yang membentuk inti konfidentialitas data fungsi f8 dan fungsi integritas data f9 dikenal sebagai KASUMI. Kondisi-kondisi berikut yang harus dipenuhi ketika mengembangkan suatu algoritma enkripsi telah digambarkan oleh Konsorsuim Third Generation Partnership Project (3GPP), yang meneliti standard teknis untuk W-Cdma, meliputi:

- Keamanan harus dipelihara di bawah spesifikasi terbuka.
- Mempaketkan pembatasan di dalam telepon mobile yang berarti bahwa algoritma itu harus diterapkan dalam perangkat keras menggunakan tidak lebih dari 10K gerbang.
- Mempertimbangkan trafik W-Cdma, yang berarti bahwa pengolahan harus pada 2Mbps.

Karena pengembangan algoritma itu hanya berlaku dalam waktu enam bulan, hal itu telah diputuskan untuk bekerja pada suatu algoritma enkripsi yang telah ada tidak untuk kembangkan suatu algoritma baru dari awal. Suatu pencarian algoritma enkripsi yang telah ada memenuhi kebutuhan itu seperti diuraikan di atas menunjukkan bahwa satu-satunya yang tersedia adalah MISTY, algoritma pada Mitsubishi Electric Corporation, KASUMI telah dikembangkan berdasarkan pada mengerjakan kembali Algoritma MISTY.

5. Kesimpulan

Dari kajian yang dilakukan terhadap keamanan jaringan CDMA, terutama CDMA2000 dan WCDMA, diperoleh beberapa kesimpulan:

1. Jaringan CDMA dengan segala kelebihannya harus diimbangi dengan teknologi keamanan mumpuni yang mencakup aspek-aspek utama pengamanan jaringan *mobile* yaitu otentifikasi dan enkripsi, proteksi data , dan proteksi sinyal.

2. Teknologi CDMA mempersulit penyadapan, baik yang bersifat terus menerus maupun sesaat karena mengimplementasikan 42-bit PN (*Pseudo-Random Noise*) sekuens yang disebut dengan “Long Code”.

3. Koordinasi lintas batas antar operaotr CDMA dan juga antara operator CDMA dengan operator seluler lainnya perlu dioptimalkan demi penggunaan spekturm yang lebih efektif dan tingkat keamanan yang lebih tinggi.

4. Keamanan jaringan CDMA pada generasi ketiga (WCDMA) sudah mengalami banyak penigkatan dibanding keamanan pada generasi kedua (CDMA2000), yang masih belum aman dilihat dari sudah dipecahkannya algoritma-algoritma yang dipakai.

5. Tidak ada sistem yang benar-benar aman. Optimasi algoritma, perbaikan mekanisme keamanan dan evaluasi harus selalu dilakukan, apapun sistem keamanannya

DAFTAR PUSTAKA

[1] Andriani, Irene. (2003). Keamanan Informasi pada CDMA2000. Institut Teknologi Bandung.

[2] Balani, Amit. (2005). Authentication and Encryption in CDMA Systems. LG Soft India.

[3] Gong, G. (2005). Encryption in Wireless Systems.

[4] Millan, William. (2005). Improved Attack on the Cellular Authentication and Encryption Algorithm. Queensland University of Technology.

[5] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[6] Naidu, Mullaguru. (2005). Cross-Border Interference Issues in CDMA Networks. Qualcomm.

[7] Palunsu, Jenny. (2004). Kajian Sistem Keamanan Jaringan 3G dan CDMA2000 1x EV-DV. Institut Teknologi Bandung.

[8] Schneier, Bruce. (1996). Applied Cryptography 2nd. John Wiley & Sons.

[9] Stojmenovic, Ivan. (2005). Cellular Networks. University of Ottawa.

[10] Wagner, David. (1999). Cryptanalysis of Cellular Message Encryption Algorithm. University of Berkeley.

[11] Wagner, David. (1999). Cryptanalysis of ORYX. University of Berkeley.

[12] Wingert, Christopher. (2002). CDMA 1x Security Oveview. Qualcomm.