UNIVERSITAS INDONESIA

ANALISIS SISTEM KEAMANAN UNTUK MOBILE WIMAX

SKRIPSI

SJAIFUL RIJAL
06 06 04 2916

FAKULTAS TEKNIK UNIVERSITAS INDONESIA
PROGRAM STUDI TEKNIK ELEKTRO
DEPOK
DESEMBER 2008

UNIVERSITAS INDONESIA

ANALISIS SISTEM KEAMANAN UNTUK MOBILE WIMAX

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana teknik

SJAIFUL RIJAL
06 06 04 2916

FAKULTAS TEKNIK UNIVERSITAS INDONESIA
PROGRAM STUDI TEKNIK ELEKTRO
DEPOK
DESEMBER 2008

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar.

Nama	: Sjaiful Rijal
NPM	: 0606042916
Tanda Tangan	:
Tanggal	: 22 Desember 2008

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :
Nama : SJAIFUL RIJAL
NPM : 0606042916
Program Studi : Teknik Elektro
Judul Skripsi : ANALISIS SISTEM KEAMANAN UNTUK MOBILE WIMAX

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Elektro, Fakultas Teknik, Universitas Indonesia

DEWAN PENGUJI

Pembimbing : Dr. Ir. Muhammad Asvial, M.Eng (.....)

Penguji : Ir. Gunawan Wibisono, M.Sc., PhD (.....)

Penguji : Fitri Yuli Zulkifli, ST., M.Sc. (.....)

Ditetapkan di : Depok

Tanggal : 22 Desember 2008

UCAPAN TERIMA KASIH

Puji syukur saya panjatkan kepada Allah SWT, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan skripsi ini. Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik pada Departemen Teknik Elektro Fakultas Teknik Universitas Indonesia. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan skripsi ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

(1) Dr. Ir. Muhammad Asvial, M..Eng, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan skripsi ini.

(2) Ibu tercinta, yang tak terhitung cinta kasihnya, hanya inilah yang bisa saya berikan untuk kado di hari ibu tahun ini. Bapak, atas dedikasinya pada pendidikan saya serta kakak, adik dan seluruh keluarga atas dukungannya yang tak pernah berhenti.

(3) Sahabat-sahabat setia dan saudara seperjuangan : Taqin, DAS, Awan, teman-teman seluruh angkatan beserta segenap civitas akademika Universitas Indonesia.

(4) Berbagai elemen baik di dunia nyata maupun dunia maya yang telah memberikan inspirasi, motivasi dan apresiasi yang teramat banyak untuk saya sebutkan satu-persatu

Akhir kata, saya berharap Allah SWT berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 22 Desember 2008

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Sjaiful Rijal
NPM : 0606042916
Program Studi : Teknik Elektro
Departemen : Teknik Elektro
Fakultas : Teknik
Jenis karya : Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :

Analisis Sistem Keamanan Untuk Mobile WiMax

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 22 Desember 2008
Yang menyatakan

(Sjaiful Rijal)

ABSTRAK

Nama : Sjaiful Rijal
Program Studi : Teknik Elektro
Judul : Analisis Sistem Keamanan Untuk Mobile WiMax

Untuk memenuhi peningkatan kebutuhan atas jaringan komunikasi wireless, IEEE mengeluarkan standard 802.16 WiMax yang mampu memberikan layanan dengan jangkauan yang luas, data rate yang tinggi dan mobilitas pengguna. Namun, selain jangkauan dan kecepatan data, privasi dan keamanan juga merupakan kebutuhan yang harus diperhatikan dalam teknologi jaringan telekomunikasi. Diantaranya yaitu untuk menjaga kerahasiaan informasi pengguna dan mencegah penggunaan layanan tanpa hak. Dalam penulisan skripsi ini akan dibahas mengenai analisis prinsip kerja sistem keamanan pada Mobile WiMax tersebut. Pada arsitektur protokol WiMax, sistem keamanan berada pada MAC layer, tepatnya pada *security sublayer*. Penulisan skripsi ini membahas proses authentikasi dan pemebentukan koneksi antara SS dengan BS, struktur MAC Protocol Data Unit serta beberapa teknik pengamanan. Dari pengujian, analisis dan program simulasi, sistem Mobile WiMax di PT. CSM menggunakan teknik pengamanan melalui pengenalan sertifikasi digigital X.509, autentikasi EAP-TTLS dan enkripsi AES-128.

Kata kunci : mobile wimax, mac-layer, sistem keamanan, enkripsi

ABSTRACT

Name : Sjaiful Rijal
Study Program : Electronical Engineering
Title : Security System Analysis For Mobile WiMax

In order to fulfill the requirement of wireless communication network, IEEE has released 802.16 standard (WiMax) that able to provide capacious range and high data rate. However, beside high bandwidth and wide-area access, privacy and security is the aspects that been concerned in the telecommunication network technology. The paper describes the analysis of security system principle in mobile WiMax. WiMax protocol architecture describes security system at MAC Layer especially security sub layer. This paper describes authentication process and connection establish between SS and BS, MAC Protocol Data Unit Structure and some protection technique. Refer to the test, analysis and simulation program, WiMax System that used in PT. CSM using security system with digital certificate X.509 and EAP-TTLS authentication, and AES-128 encryption.

Keywords : mobile wimax, mac-layer, security system, encryption

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB 1

PENDAHULUAN

1.1. LATAR BELAKANG

Seiring dengan berkembangnya kebutuhan komunikasi data dan internet, maka berkembang pula teknologi jaringan telekomunikasi. Diantaranya jaringan akses dari penyedia layanan ke para pengguna layanan tersebut, yang biasa disebut juga dengan "*lastmile*".

Untuk itu IEEE mengeluarkan standard 802.16 yang diperuntukkan untuk jaringan MAN (*metropolitan area network*) yang kemudian diperbarui hingga 802.16e dengan menambahkan fitur mobilitas pengguna. Teknologi yang digunakan pada standard ini menggunakan frekuensi 2 hingga 11 GHz, dengan daya cakup NLoS (*Non - Line of Sight*) hingga 8 Km dengan kecepatan data hingga 75 Mbps.[1]

Dengan jangkauan yang luas dan kecepatan data yang tinggi tersebut, WiMax dapat melayani pengguna lebih banyak. Dengan demikian pengguna akan lebih mudah untuk dapat mengakses sinyal dari *Base Station* WiMax. Untuk itu diperlukan sistem keamanan yang lebih baik untuk menjamin privasi dan mengantisipasi gangguan keamanan, baik berupa pengguna yang tidak diizinkan maupun penyalahgunaan informasi pengguna layanan tersebut.

Pengaturan sistem keamanan pada sistem MobileWiMax tersebut sebagian besar dilakukan pada lapisan *mac-layer*, khususnya pada *security sublayer*. Dimana terjadi proses autentikasi dan pembentukan kunci keamanan dan enkripsi.

1.2. TUJUAN PENULISAN

Penulisan skripsi ini bertujuan untuk menganalisis prinsip kerja sistem keamanan pada *mac-layer* mobile WiMax. Yaitu bagaimana sistem WiMax mengatur penggunaan layanannya dan melindungi privasi penggunaan layanan. Dimana hal ini diatur pada lapisan *mac-layer* khususnya *security sub-layer*.

1.3. BATASAN MASALAH

Pada penulisan skripsi ini dibatasi pada :

a. Analisis prinsip dasar sistem keamanan pada mac-layer Mobile WiMax.
b. Simulasi kerja sistem enkripsi dengan menggunakan metode enkripsi *Advance Encryption System* (AES).
c. Analisis prinsip kerja sistem keamanan pada Mobile WiMax yang digunakan ole PT. Citra Sari Makmur.
d. Pada penulisan skripsi ini tidak dilakukan pengujian pada sistem selain yang digunakan di PT. CSM

1.4. SISTEMATIKA PENULISAN

Dalam penulisan skripsi ini, penyusunan dibagi dalam lima bab dan selanjutnya diperjelas dalam beberapa sub-bab. Secara keseluruhan skripsi ini disusun dalam sistematika sebagai berikut.

BAB 1 PENDAHULUAN

Berisikan latar belakang masalah, tujuan penulisan, batasan masalah, dan sistematika penulisan.

BAB 2 DASAR TEORI SISTEM KEAMANAN MOBILE WIMAX

Berisikan landasan-landasan teori yang mendasari penulisan skripsi ini. Di antaranya meliputi konsep dasar sistem komunikasi WiMax, sistem mac layer WiMax, sistem keamanan jaringan, sistem keamanan pada WiMax, enkripsi dan kriptografi.

BAB 3 PERANCANGAN DAN PEMBUATAN SISTEM

Berisikan tentang perancangan perangkat lunak untuk simulasi sistem keamanan pada mac layer Mobile WiMax dan perencanaan pengujian sistem keamanan Mobile WiMax di PT. Citra Sari Makmur.

BAB 4 PENGUJIAN DAN ANALISIS

Berisikan tentang pengujian sistem serta analisis sistem keamanan pada mac layer Mobile Wimax..

BAB V PENUTUP

Berisikan tentang kesimpulan dari penulisan skripsi yang berjudul "Analisis Sistem Keamanan Untuk Mobile WiMax".

BAB 2

DASAR TEORI SISTEM KEAMANAN MOBILE WIMAX

2.1. Pengenalan WiMax

Worldwide Interoperability for Microwave Access (WiMAX) merupakan evolusi dari teknologi *Broadband Wireless Access* (BWA) sebelumnya. Bila teknologi BWA sebelumnya masih *proprietary* atau berdasarkan hak cipta, maka teknologi WiMAX bersifat standard terbuka. Dalam arti komunikasi perangkat WiMAX diantara beberapa vendor yang berbeda tetap dapat dilakukan.

Pengembangan teknologi WiMAX terjadi dalam beberapa tahap atau mengalami evolusi. Sesuai dengan standarisasinya, dikatakan bahwa teknologi WiMAX diatur dalam standard IEEE 802.16. Standard ini terbagi lagi dalam beberapa kategori yaitu IEEE 802.16a yaitu untuk standard BWA yang belum open standard atau biasa disebut dengan Pre-WiMAX. Selanjutnya standard ini dikembangkan lagi menjadi standard IEEE 802.16d untuk WiMAX area tetap atau nomadik. Sementara untuk WiMAX bergerak yang disebut Mobile WiMAX akan diatur dalam standarisasi IEEE 802.16e yang telah diratifikasi pada akhir tahun 2005.

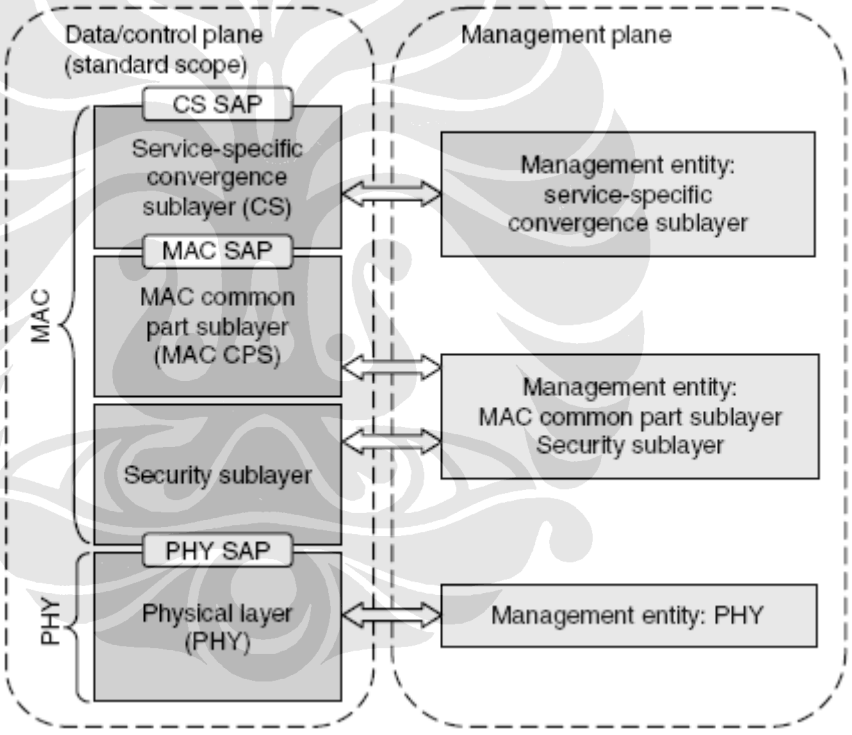
Disamping evolusi pada sisi kemampuan akses, terjadi juga evolusi pada sisi perangkat untuk pelanggan atau *Customer Premises Equipment* (CPE). Pada tahap awal, perangkat CPE WiMAX berupa perangkat untuk area tetap luar ruangan, kemudian berkembang menjadi area tetap dalam ruangan, portabel (nomadik) dan *mobile*. Perangkat untuk area tetap luar ruangan merupakan perangkat CPE terdiri dari 2 unit yaitu unit luar ruangan yang terdiri dari radio dan antena serta unit dalam ruangan yang merupakan antarmuka ke terminal pelanggan. Pada tipe area tetap dalam ruangan, perangkat CPE hanya terdiri dari satu unit perangkat dalam ruangan yang sudah terdiri dari radio, antena dan port antarmuka pengguna. Umumnya pada tipe ini, pengguna dapat menmasang sendiri perangkat CPE-nya (*self installation*).

Tahap berikutnya, perangkat CPE sudah bukan merupakan perangkat independen tetapi tergabung dalam terminal pelanggan seperti laptop dan PDA.

Pada tahap ini, CPE WiMAX portabel telah terpasang permanen pada terminal sebagaimana CPE Wi-Fi. Terakhir adalah perangkat bergerak. Keunggulan yang ditambahkan adalah kemampuan portabilitas yang lebih tinggi selain ukuran terminal yang lebih ringkas.

2.2. Lapisan Protokol WiMax

Pada WiMax/802.16 ditetapkan 2 lapisan protokol, yaitu lapisan fisik (PHY) dan lapisan *medium acces control* (MAC). Lapisan MAC mengatur masalah koneksi, Qos dan keamanan. Sedangkan lapisan PHY menangani ketersambungan sinyal dan koreksi kesalahan.



Gambar 2.1 Lapisan Protokol WiMax[1]

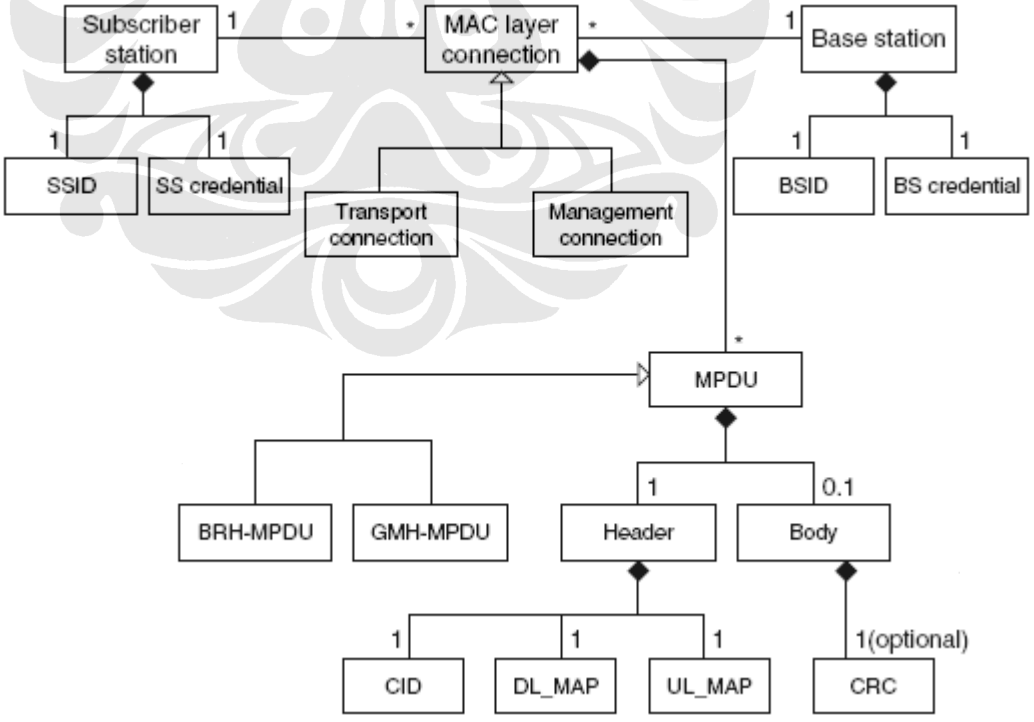
Dari lapisan MAC tersebut dapat dibagi lagi menjadi tiga sub-lapisan. Yang pertama sub-lapisan keamanan (*security sublayer*) yang berperan dalam proses autentikasi, pembentukan kunci keamanan dan enkripsi. Yang kedua adalah sub-lapisan MAC bagian umum (*MAC common part sublayer*). Dan yang ketiga adalah sub-lapisan kovergensi layanan khusus (*service-specific convergence*

sublayer). Sub Lapisan ini berhubungan langsung dengan lapisan diatasnya yang lebih tinggi.

2.3. Aspek Jaringan

Setiap stasiun pelanggan atau SS (*subscriber station*) berkomunikasi dengan stasiun utama atau BS (*base station*) melalui sambungan nirkabel. Sebelum tersambung, SS memindai daftar frekuensi-frekuensinya untuk mencari sinyal dari BS. Kemudian megobservasi trafik dari BS tersebut untuk menentukan parameter-parameter seperti perjangkaan, modulasi, koreksi kesalahan dan daya. Kemudian yang terakhir mengidentifikasi *timeslot* yang akan digunakan untuk melakukan *initial request*.

Rangkain paket-paket *initial* (*ranging request*) tersebut memperbaiki pengaturan perjangkaan dan daya, serta membentuk reservasi koneksi dengan menentukan profil celah waktu (*timeslot)* dan identitas koneksi (CID). BS memberikan bermacam CID yang berbeda kepada SS untuk tiap managemen, koneksi data dan kualitas layanan atau *Quality of Service* (QoS) yang berbeda.

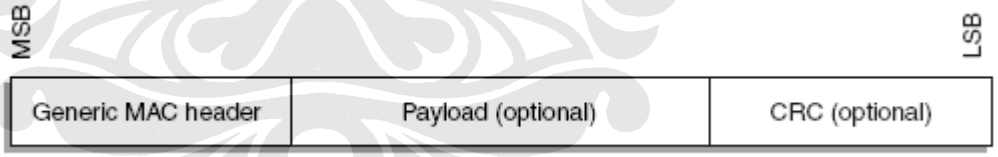


Gambar 2.2 Arsitektur Jaringan WiMax

Kominikasi antara SS dan BS dibagi menjadi kerangka-kerangka. Kerangka dari BS menuju SS disebut *downlink frames*. Sedangkan kerangka dari SS menuju BS disebut *uplink frames*. Kerangka-kerangka tersebut terdiri berisi tajuk kerangka (*frame header*) dan tubuh kerangka (*body)*. Tajuk dari tiap-tiap kerangka tersebut memiliki dua jenis pemetaan atau *map* yang menggambarkan penggunaan celah beserta penempatannya, yaitu *downlink map* (DL_MAP) dan *uplink map* (UL_MAP). Dan tiap-tiap celah tersebut merupakan bagian dari beberapa koneksi yang diidentifikasi oleh CID. [1]

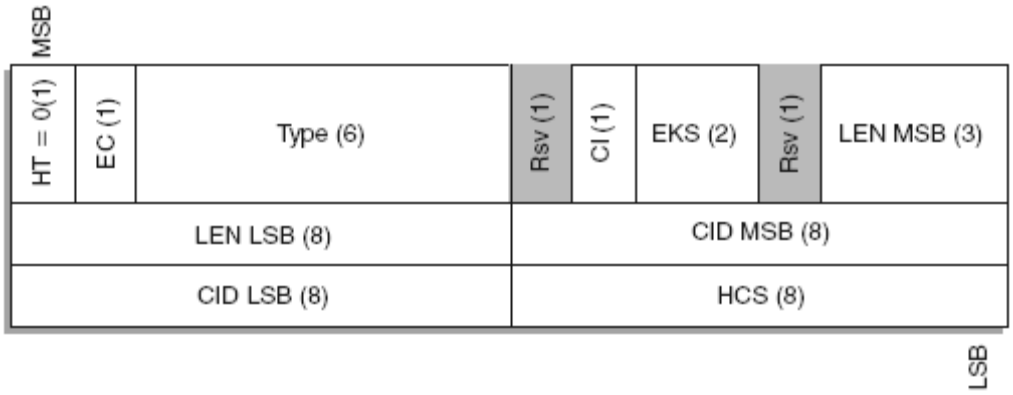
2.4. MAC Protocol Data Unit (MPDU)

Tiap-tiap *protocol data unit* (PDU) terdiri atas *generic MAC headaer* (GMH), *payload,* dan cyclic redundancy check (CRC) yang bersifat opsional. GMH menunjukkan kandungan dari payload dan dimulai dari most significant bit (MSB). Payload itu sendiri berisi nol atau lebih subheader dan MAC *service data unit* (SDU). Panjang dari payload tersebut dapat bermacam-macam. CRC bersifat opsional pada PHY layer tipe SC, namun merupakan keharusan untuk PHY layer tipe SCa, OFDM, dan OFDMA. [1]



Gambar 2.3 MAC PDU

Terdapat dua format yang ditetapkan untuk MAC *header*. Yaitu GMH yang yang digunakan untuk MAC PDU yang berisi pesan manajemen MAC atau data sub-lapisan konvergen. Berikutnya adalah *Bandwidth Request Header* (BRH) yang digunakan ketika melakukan permintaan bandwidth tambahan. Kedua jenis *header* tersebut dibedakan oleh satu bit "*header type*" (HT). Dimana berisi 0 untuk generic header dan berisi satu untuk bandwidth request header.

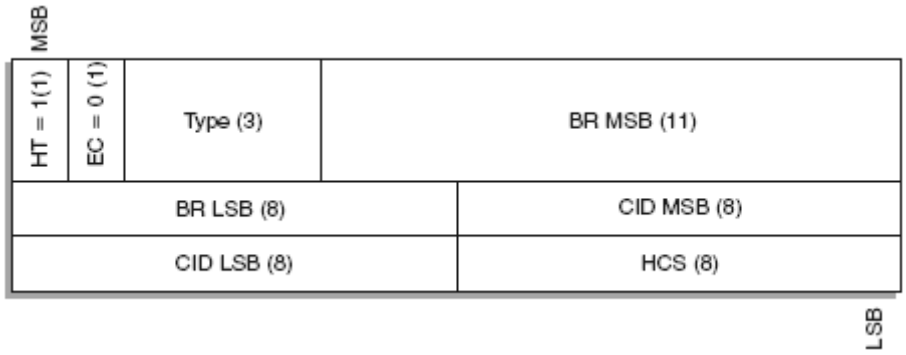


Gambar 2.4 Generic MAC Header

Pada Gambar2.4, merupakan MAC *header* jenis GMH. Hal ini ditunjukkan pada field HT yang berisi "0". Panjang dari GMH ini adalah 6 byte dan terdiri atas 12 field. Dimana isi dari masing-masing field tersebut akan dijelaskan tabel berikut :

Tabel 2.1 Field-field GMH

Name	Length (Bits)	Description
CI	1	CRC indicator 1 = CRC is included in the PDU by appending it to the payload after encryption if any 0 = No CRC is included
CID	16	Connection identifier
EC	1	Encryption control 0 = Payload is not encrypted 1 = Payload is encrypted
EKS	2	Encryption key sequence The index of the traffic encryption key (TEK) and initialization vector used to encrypt the payload. This field is only meaningful if the EC field is set to 1
HCS	8	Header check sequence An 8-bit field used to detect errors in the header
HT	1	Header type Shall be set to zero
LEN	11	Length The length in bytes of the MAC PDU including the MAC header and the CRC if present
Type	6	This field indicates the subheaders and special payload types present in the message payload



Gambar 2.5 Struktur BRH PDU

Sedangkan PDU tipe *bandwidth request* tidak memiliki *payload*, melainkan hanya terdiri atas *header* saja. Panjang dari *header* tersebut adalah sama dengan GMH yaitu 6 byte, namun hanya terdiri atas 8 field. Dimana isi dari masing-masing field tersebut akan dijelaskan tabel berikut :

Tabel 2.2 Field-field BRH

Bandwidth Request Header Fields

Name	Length (Bits)	Description
BR	19	Bandwidth request The number of bytes of uplink bandwidth requested by the subscriber station. The bandwidth request is for the CID. The request shall not include any PHY overhead
CID	16	Connection identifier
EC	1	Always set to zero
HCS	8	Header check sequence An 8-bit field used to detect errors in the header
HT	1	Header type = 1
Type	3	Indicates the type of bandwidth request header

2.5. Security Association (SA)

Security association (SA) merupakan seperangkat metode kriptografi dan asosiasi penyandian yang terdiri dari informasi tentang bagaimana penerapan suatu algoritma, bagaimana menggunakan penyandian dan lainsebagainya.

Setiap pelayanan memerlukan asosiasi keamanan. Untuk stasiun pelanggan (SS) menggunakan *traffic encryption* (TEK) *state machine* untuk setiap asosiasi keamanan. TEK akan bertanggung jawab untuk memanajemen enkripsi lalu lintas data pada setiap pelayanan. Subscriber station (SS) akan mengirimkan key request

ke base station (BS), dan base station (BS) akan mengirimkan jawaban secara random private key ke subscriber station (SS). Kunci ini dienkripsi menggunakan 3DES selama proses authorization.

Setelah dienkripsi menggunakan kunci private, maka semua data dienkripsi dengan algoritma kunci simetrik. Spesifikasi yang digunakan adalah 56-bit DES dalam mode cyclic block chaining(CBC). Ada tiga tipe security association (SA) yaitu primary, static dan dynamic. Setiap subscriber station (SS) menentukan sebuah primary security association (SA) dengan base station (BS) selama proses inisialisasi. Static security association ditentukan oleh base station (BS), sedangkan dynamic security association ditentukan dan diselesaikan oleh setiap permulaan dan akhir layanan selama proses koneksi. Setiap subscriber station (SS) mempunyai nomor yang unik dan eklusif, tetapi semua tipe static dan dynamic dapat di-share dengan multiple subscriber station. Subscriber station (SS) bertanggung jawab untuk menanyakan kepada base station (BS) untuk substansi yang baru sebelum waktunya habis pada base station(BS). Protokol PKM juga bertanggung jawab terhadap sinkronisasi antara subscriber station (SS) dan base station (BS).

2.6. Kriptografi

Kriptografi berasal dari dua kata Yunani, yaitu *Crypto* yang berarti rahasia dan *Grapho* yang berarti menulis. Secara umum kriptografi dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu pesan. Kriptografi pada dasarnya sudah dikenal sejak lama. Menurut catatan sejarah, kriptografi sudah digunakan oleh bangsa Mesir sejak 4000 tahun yang lalu oleh raja-raja Mesir pada saat perang untuk mengirimkan pesan rahasia kepada panglima perangnya melalui kurir-kurinya. Orang yang melakukan penyandian ini disebut *kriptografer*, sedangkan orang yang mendalami ilmu dan seni dalam membuka atau memecahkan suatu algoritma kriptografi tanpa harus mengetahui kuncinya disebut *kriptanalis*.

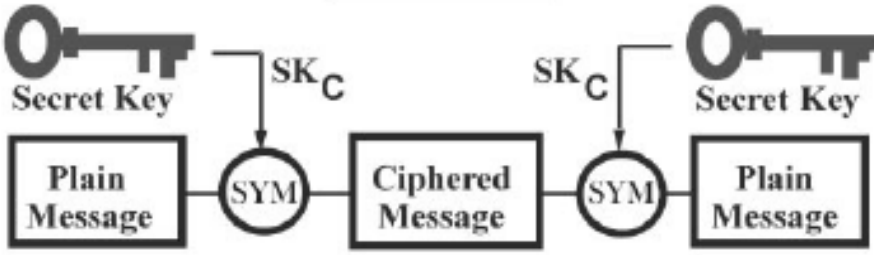
Seiring dengan perkembangan teknologi, algoritma kriptografi pun mulai berubah menuju ke arah algoritma kriptografi yang lebih rumit dan kompleks.

Kriptografi mau tidak mau harus diakui mempunyai peranan yang paling penting dalam peperangan sehingga algoritma kriptografi berkembang cukup pesat pada saat Perang Dunia I dan Perang Dunia II. Menurut catatan sejarah, terdapat beberapa algoritma kriptografi yang pernah digunakan dalam peperangan, diantaranya adalah ADFVGX yang dipakai oleh Jerman pada Perang Dunia I, *Sigaba/M-134* yang digunakan oleh Amerika Serikat pada Perang Dunia II, *Typex* oleh Inggris, dan *Purple* oleh Jepang. Selain itu Jerman juga mempunyai mesin legendaris yang dipakai untuk memecahkan sandi yang dikirim oleh pihak musuh dalam peperangan yaitu, *Enigma*.

Algoritma kriptografi yang baik tidak ditentukan oleh kerumitan dalam mengolah data atau pesan yang akan disampaikan. Yang penting, algoritma tersebut harus memenuhi 4 persyaratan berikut :

- Kerahasiaan. Pesan (*plaintext*) hanya dapat dibaca oleh pihak yang memliki kewenangan.
- Autentikasi. Pengirim pesan harus dapat diidentifikasi dengan pasti, penyusup harus dipastikan tidak bisa berpura-pura menjadi orang lain.
- Integritas. Penerima pesan harus dapat memastikan bahwa pesan yang dia terima tidak dimodifikasi ketika sedang dalam proses transmisi data.
- ***Non-Repudiation***. Pengirim pesan harus tidak bisa menyangkal pesan yang dia kirimkan.

Kriptografi pada dasarnya terdiri dari dua proses, yaitu proses enkripsi dan proses dekripsi. Proses enkripsi adalah proses penyandian pesan terbuka menjadi pesan rahasia (ciphertext). Ciphertext inilah yang nantinya akan dikirimkan melalui saluran komunikasi terbuka. Pada saat ciphertext diterima oleh penerima pesan, maka pesan rahasia tersebut diubah lagi menjadi pesan terbuka melalui proses dekripsi sehingga pesan tadi dapat dibaca kembali oleh penerima pesan. Secara umum, proses enkripsi dan dekripsi dapat digambarkan sebagai berikut :



Gambar 2.6 Gambar Proses Enkripsi dan Dekripsi[4]

Dalam sistem komputer, pesan terbuka (*plaintext*) diberi lambang M, yang merupakan singkatan dari *Message*. *Plaintext* ini dapat berupa tulisan, foto, atau video yang berbentuk data biner. *Plaintext* inilah yang nantinya akan dienkripsi menjadi pesan rahasia atau *ciphertext* yang dilambangkan dengan C (*Ciphertext*). Secara matematis, fungsi enkripsi ini dinotasikan dengan :

$$E(M) = C$$

Sedangkan fungsi dekripsi adalah proses pembalikan dari *ciphertext* menjadi *plaintext* kembali. Secara matematis dinotasikan sebagai berikut :

$$D(C) = M$$

$$D(E(M)) = M$$

2.6.1. Panjang Kunci

Keamanan dari sebuah teknik penyandian tergantung dari dua hal : algoritma penyandian dan panjang kunci (*key*). Algoritma sangat menentukan kekuatan dari sebuah teknik penyandian, tetapi panjang kunci juga tidak kalah penting dalam menentukan kekuatan sebuaBh teknik penyandian.

Sebagai contoh, apabila seorang *kriptanalis* mengetahui algoritma yang dipakai untuk melakukan teknik penyandian terhadap suatu pesan, maka *kriptanalis* tersebut harus mendapatkan kunci yang dipakai terlebih dahulu sebelum dapat melakukan dekripsi terhadap semua *ciphertext* yang dia punya. Satu-satunya cara untuk mendapatkan kunci yang dipakai adalah dengan cara mencoba semua variasi kunci yang ada. Teknik serangan ini sering dikenal dengan nama *brute force.*

Adalah mudah untuk menghitung banyaknya variasi kunci yang ada. Apabila panjang kunci adalah 8 bit, maka ada 2^8 atau 256 kemungkinan kunci yang dapat dicoba. Dari 256 percobaan ini, peluang untuk mendapatkan kunci yang benar adalah 50 persen setelah melalui setengah usaha percobaan. Bila panjang kunci 56 bit, maka ada 2^{56} kemungkinan variasi kunci. Dengan menganggap sebuah superkomputer dapat mencoba satu juta kunci per detik, maka diperkirakan sekitar 2285 tahun untuk menemukan kunci yang benar. Bila menggunakan panjang kunci 64 bit, maka dengan superkomputer yang sama akan membutuhkan 585 ribu tahun. Dengan jangka waktu yang lama ini, maka dapat dipastikan bahwa pesan yang disandikan tersebut tidak mempunyai arti lagi apabila telah berhasil dilakukan dekripsi.

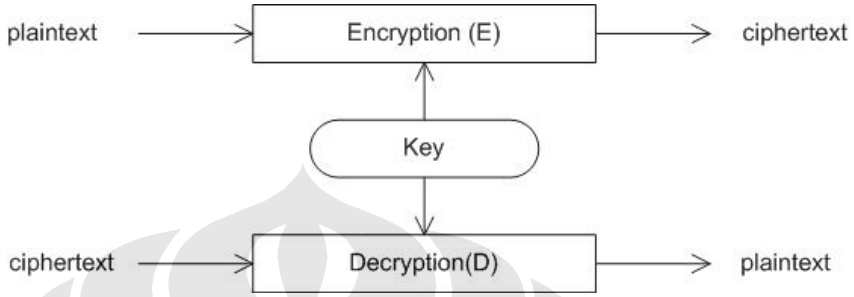
Dengan melihat situasi ini, maka kriptografi yang baik akan memilih untuk menggunakan sepanjang mungkin kunci yang akan digunakan, namun hal ini tidak dapat diterapkan begitu saja. Semakin panjang kunci, semakin lama pula waktu yang digunakan oleh komputer untuk melakukan proses enkripsi. Oleh sebab itu, panjang kunci yang akan digunakan hendaknya memperhatikan 3 hal, yaitu seberapa penting data yang akan dirahasiakan, berapa lama waktu yang dibutuhkan agar data tersebut tetap aman, dan seberapa kuat kemampuan *kriptanalis* dalam memecahkan teknik penyandian kita. Saat ini yang paling banyak dipakai adalah kunci dengan panjang 128 bit karena panjang kunci ini dianggap paling optimal untuk saat ini.

2.6.2. Kriptografi Kunci Rahasia dan Kunci Publik

Pada dasarnya terdapat dua jenis algoritma kriptografi berdasarkan kunci yang digunakan. Yang pertama adalah kriptografi dengan menggunakan secret key dan yang kedua adalah kriptografi yang menggunakan public key. Kriptografi public key menggunakan dua kunci yang berbeda dimana satu kunci digunakan untuk melakukan enkripsi dan kunci yang lain digunakan untuk melakukan dekripsi.

2.6.2.1. Kriptografi Kunci Rahasia

Kriptografi kunci rahasia atau *secret key* adalah kriptografi yang hanya melibatkan satu kunci dalam proses enkripsi dan dekripsi. Proses dekripsi dalam kriptografi *secret key* ini adalah kebalikan dari proses enkripsi.



Gambar 2.7 Kriptografi simetris

Kriptografi *secret key* seringkali disebut sebagai kriptografi konvensional atau kriptografi simetris (*Symmetric Cryptography*) dimana proses dekripsi adalah kebalikan dari proses enkripsi dan menggunakan kunci yang sama.

Kriptografi simetris dapat dibagi menjadi dua, yaitu penyandian blok dan penyandian alir. Penyandian blok bekerja pada suatu data yang terkelompok menjadi blok-blok data atau kelompok data dengan panjang data yang telah ditentukan. Pada penyandian blok, data yang masuk akan dipecah-pecah menjadi blok data yang telah ditentukan ukurannya. Penyandian alir bekerja pada suatu data bit tunggal atau terkadang dalam satu byte. Jadi format data yang mengalami proses enkripsi dan dekripsi adalah berupa aliran bit-bit data.

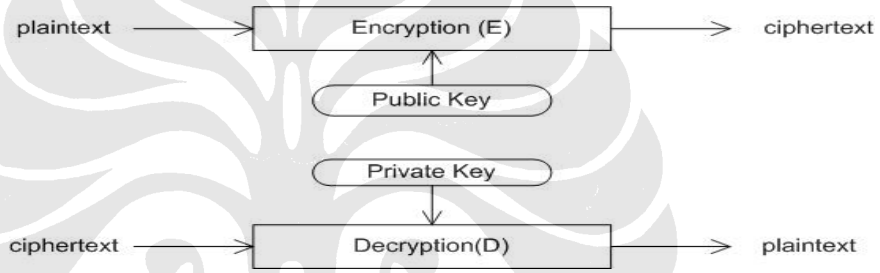
Algoritma yang ada pada saat ini kebanyakan bekerja untuk penyandian blok karena kebanyakan proses pengiriman data pada saat ini menggunakan blok-blok data yang telah ditentukan ukurannya untuk kemudian dikirim melalui saluran komunikasi.

2.6.2.2. Kriptografi Kunci Publik

Kriptografi *public key* sering disebut dengan kriptografi asimetris. Berbeda dengan kriptografi *secret key*, kunci yang digunakan pada proses enkripsi dan

proses dekripsi pada kriptografi public key ini berbeda satu sama lain. Jadi dalam kriptografi *public key*, suatu *key generator* akan menghasilkan dua kunci berbeda dimana satu kunci digunakan untuk melakukan proses enkripsi dan kunci yang lain digunakan untuk melakukan proses dekripsi.

Kunci yang digunakan untuk melakukan enkripsi akan dipublikasikan kepada umum untuk dipergunakan secara bebas. Oleh sebab itu, kunci yang digunakan untuk melakukan enkripsi disebut juga sebagai *public key*. Sedangkan kunci yang digunakan untuk melakukan dekripsi akan disimpan oleh pembuat kunci dan tidak akan dipublikasikan kepada umum. Kunci untuk melakukan dekripsi ini disebut *private key*.



Gambar 2.8 Kriptografi Asimetris

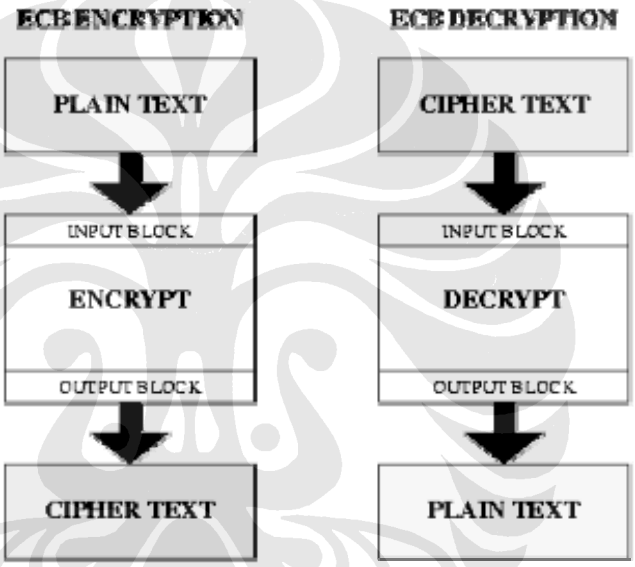
Dengan cara demikian, semua orang yang akan mengirimkan pesan kepada pembuat kunci dapat melakukan proses enkripsi terhadap pesan tersebut, sedangkan proses dekripsi hanya dapat dilakukan oleh pembuat atau pemilik kunci dekripsi. Dalam kenyataannya, kriptografi asimetris ini dipakai dalam ssh, suatu layanan untuk mengakses suatu server.

2.6.3. Penyandian Blok

Penyandian blok pada dasarnya adalah proses penyandian terhadap blok data yang jumlahnya sudah ditentukan. Untuk sistem penyandian blok terdapat empat jenis mode operasi, yaitu *Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB).*

2.6.3.1. Electronic Code Book (ECB)

Mode ECB adalah mode yang paling umum dan paling mudah untuk diimplementasikan. Cara yang digunakan adalah dengan membagi data ke dalam blok-blok data terlebih dahulu yang besarnya sudah ditentukan. Blok-blok data inilah yang disebut *plaintext* karena blok data ini belum disandikan. Proses enkripsi akan langsung mengolah *plaintext* menjadi *ciphertext* tanpa melakukan operasi tambahan. Suatu blok *plaintext* yang dienkripsi dengan menggunakan kunci yang sama akan menghasilkan *ciphertext* yang sama.



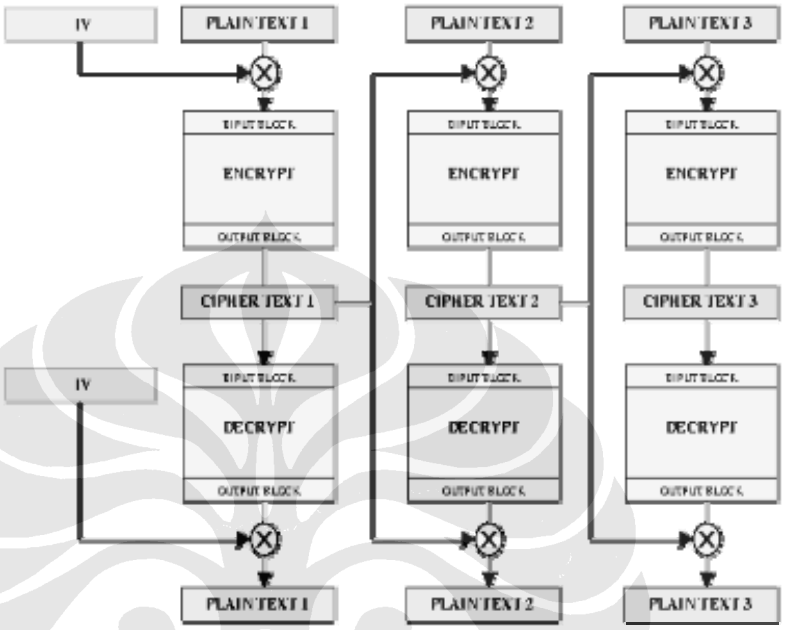
Gambar 2.9 Mode Operasi ECB

Keuntungan dari mode OBC ini adalah kemudahan dalam implementasi dan pengurangan resiko salahnya semua *plaintext* akibat kesalahan pada satu *plaintext*. Namun mode ini memiliki kelemahan pada aspek keamanannya. Dengan mengetahui pasangan *plaintext* dan *ciphertext*, seorang *kriptanalis* dapat menyusun suatu *code book* tanpa perlu mengetahui kuncinya.

2.6.3.2. Cipher Block Chaining (CBC)

Pada CBC digunakan operasi umpan balik atau dikenal dengan operasi berantai (*chaining*). Pada CBC, hasil enkripsi dari blok sebelumnya adalah

feedback untuk enkripsi dan dekripsi pada blok berikutnya. Dengan kata lain, setiap blok *ciphertext* dipakai untuk memodifikasi proses enkripsi dan dekripsi pada blok berikutnya.

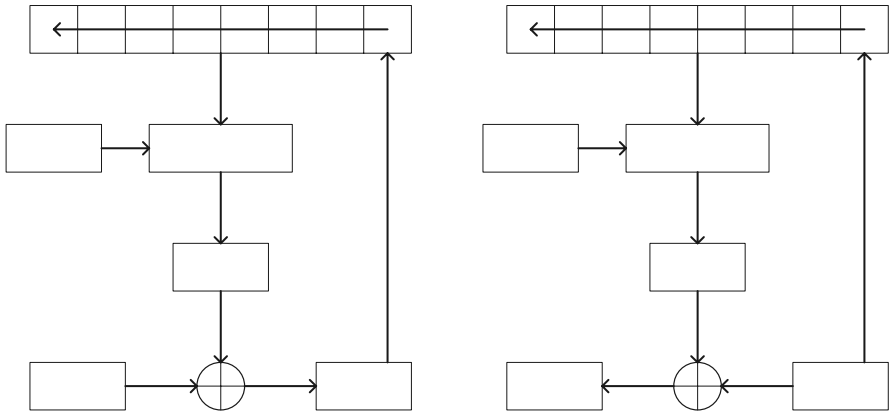


Gambar 2.10 Mode Operasi CBC

Pada CBC diperlukan data acak sebagai blok pertama. Blok data acak ini sering disebut *initialization vector* atau IV. IV digunakan hanya untuk membuat suatu pesan menjadi unik dan IV tidak mempunyai arti yang penting sehingga IV tidak perlu dirahasiakan.

2.6.3.3. Cipher Feedback (CFB)

Pada mode CBC, proses enkripsi atau dekripsi tidak dapat dilakukan sebelum blok data yang diterima lengkap terlebih dahulu. Masalah ini diatasi pada mode *Cipher Feedback* (CFB). Pada mode CFB, data dapat dienkripsi pada unit-unit yang lebih kecil atau sama dengan ukuran satu blok. Misalkan pada CFB 8 bit, maka data akan diproses tiap 8 bit.



Gambar 2.11 Mode Operasi CFB

Pada permulaan proses enkripsi, IV akan dimasukkan dalam suatu *register* geser. IV ini akan dienkripsi dengan menggunakan kunci yang sudah ada. Dari hasil enkripsi tersebut, akan diambil 8 bit paling kiri atau *Most Significant Bit* untuk di-XOR dengan 8 bit dari *plaintext*. Hasil operasi XOR inilah yang akan menjadi *ciphertext* dimana *ciphertext* ini tidak hanya dikirim untuk ditransmisikan tetapi juga dikirim sebagai *feedback* ke dalam *register* geser untuk dilakukan proses enkripsi untuk 8 bit berikutnya.

Kunci

2.6.3.4. Output Feedback (OFB)

Sama pada mode CFB, mode OFB juga memerlukan sebuah *register* geser dalam pengoperasiannya. Pertama kali, IV akan masuk ke dalam *register* geser dan dilakukan enkripsi terhadap IV tersebut. Dari hasil proses enkripsi tersebut akan diambil 8 bit paling kiri untuk dilakukan XOR dengan *plaintext* yang nantinya akan menghasilkan *ciphertext*. *Ciphertext* tidak akan diumpan balik ke dalam *register* geser, tetapi yang akan diumpan balik adalah hasil dari enkripsi IV.

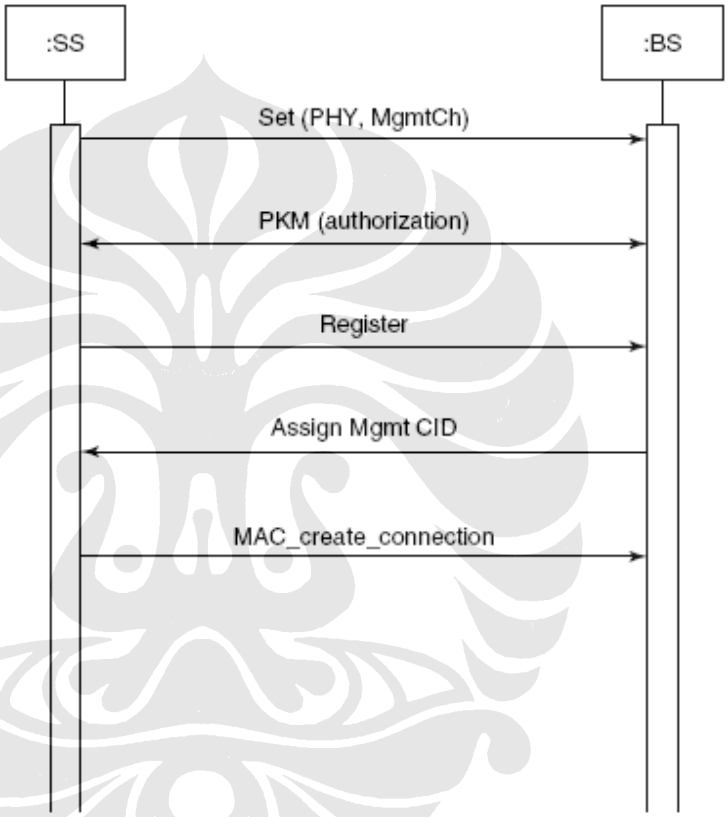
2.7. Proses Pengamanan

2.7.1. Memulai Koneksi

P(n)

Unuk memulai suatu koneksi antara SS dngan BS, dilakukan melalui beberapa tahapan. Tahapan paling awal yang harus dilakukan adalah pada layer

PHY. SS melakukan pemindaian signal untuk mengetahui keberadaan BS yang terdekat. Kemudian megobservasi trafik dari BS tersebut untuk menentukan parameter-parameter seperti timing, modulasi, error correction dan power. Kemudian yang terakhir mengidentifikasi timeslot yang akan digunakan untuk melakukan initial request. Dengan begitu SS dapat membentuk channel yang akan digunakan untuk meminta autorisasi dari BS.



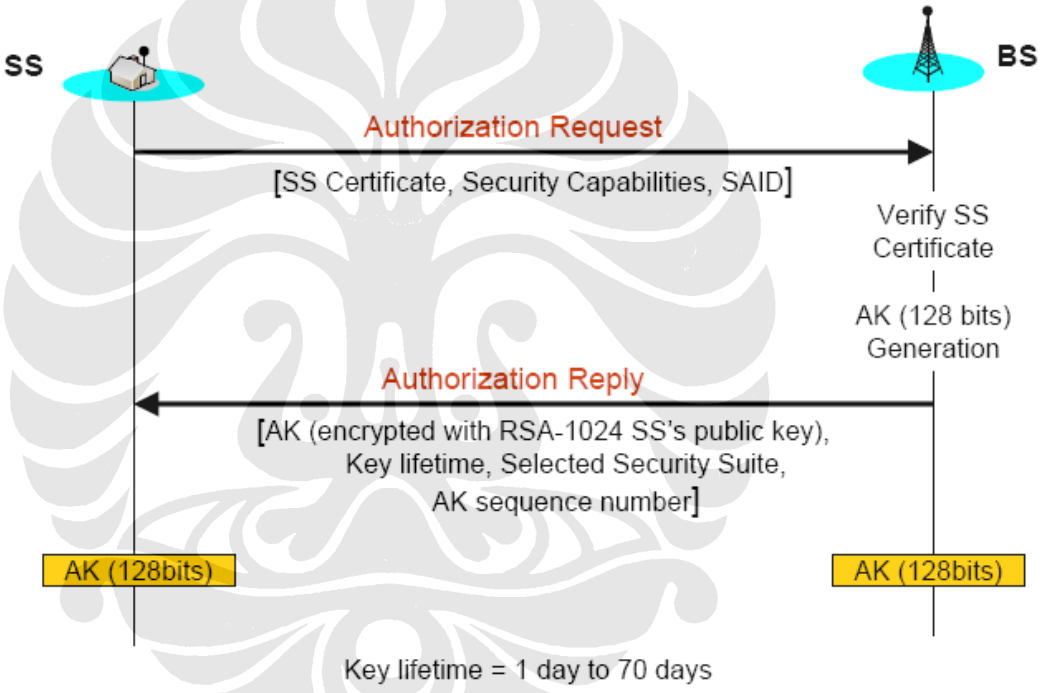
Gambar 2.12 Proses koneksi[2]

Bila telah mendapatkan alokasi channel, SS akan meminta autorsasi pada BS. SS mengirimkan permintaan tersebut dengan menyeertakan MAC address dan sertifikasi dari pabrikan pembuatnya.

Bila MAC address dan sertifikasi yang diberikan SS sesuai dan berhak mendapatkan akses, maka BS akan memberikan autorisasi. Sehingga kemudian SS dapat melakukan registrasi untuk mendapatkan management CID yang akan digunakan untuk membentuk koneksi antara SS dan BS sesuai dengan haknya.

2.7.2. Autentikasi

Untuk menentukan SS berhak membentuk koneksi atau tidak, dilakukan melalui proses auentikasi. SS memulai proses autorisasi dengan mengirimkan informasi autentikasi kepada BS yang dituju. Informasi tersebut berisi sertifikasi X.509 yang dikeluarkan oleh pabrikan yang bersangkutan atau badan otoritas lainnya. Setela mengirim informasi autentikasi tersebut, SS juga segera mengirimkan authirization request untuk meminta key autentikasi. Detail proses autentikasi tersebut digambarkan melalui Gambar 2.13 berikut :



Gambar 2.13 Proses Autentikasi[3]

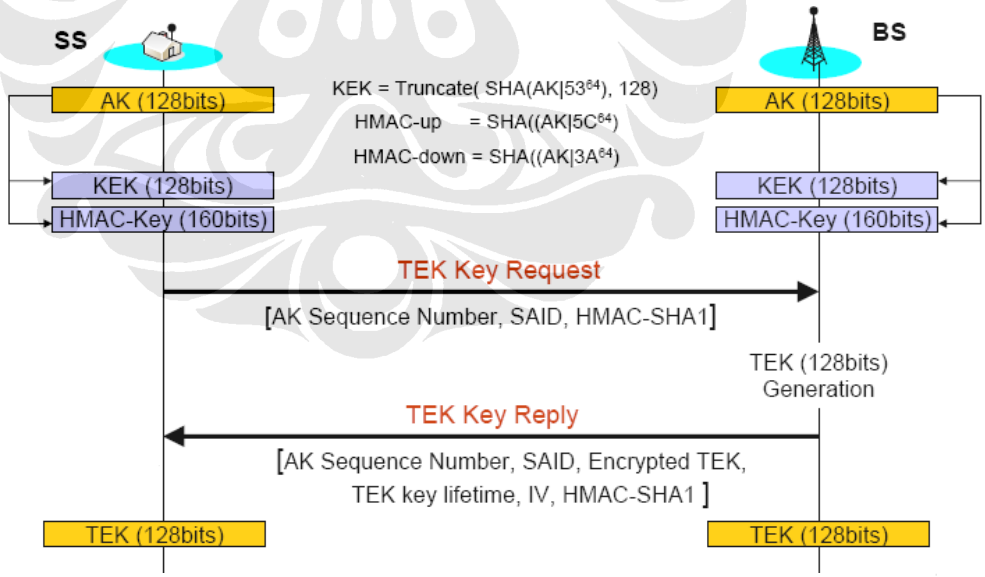
Seperti yang terilustrasi dalam Gambar 2.13, SS menginformasikan pada BS SAID-nya. BS melakukann validasi terhadap identitas SS yang melakukan permintaan. Setelah melakukan verifikasi terhadap identitas SS tersebut, BS mengaktifkan sebuah authentication key (AK) untuk SS, mengenkripsinya dengan kunci publik, kemudian mengirimkannya kembali kepada SS melalui authorization reply.

Data inforasi yang dikirimkan antara SS dan BS dalam proses autentikasi ini antaralain adalah:

- Sertifikasi X.509 yang dieluarkan oleh vendor (sebagai identitas SS yang melakukan request).
- Deskripsi dari algoritma kriptografi yang didukung oleh SS (disebut sebagai security association [SA]).
- Basic CID dari SS, yang sama dengan primary SAID.

2.7.3. Pertukaran Kunci Data

Base station (BS) bertanggung jawab dalam pemeliharaan informasi untuk semua *securityassociation (SA),* sedangkan *subscriber station* (*SS)* bertanggung jawab untuk mendukung otorisasi dengan *base station (BS)* dan memelihara otorisasi kunci yang aktif. Setelah *subscriber station*(*SS)* menyelesaikan negoisasi, maka akan mengubah otorisasi dengan *base station (BS)*. Awalnya*base station (BS)* menerima pesan dari *subscriber station* (*SS)* untuk mengaktifkan otoritas yang baru, kemudian *base station (BS)* mengirimkan jawaban atas pertanyaan *subscriber station* (*SS).*



Gambar 2.14 Proses Pertukaran Key[3]

Authorization key (AK) akan aktif sampai waktu yang ditentukan berakhir sesuai dengan bataswaktu *authorization key (AK).* Apabila *subscriber station* (*SS)* mengalami kegagalan dalam melaksanakan otorisasi sebelum waktu *authorization*

key (AK) berakhir, maka *base station (BS)* tidak dapat mengaktifkan *authorization key (AK)* untuk *subscriber station* (*SS),* dan *subscriber station* (*SS)* tidak diberi otorisasi. *Base station (BS)* akan menghapus semua *traffic encryption* (*TEK)* dengan otorisasi dari *subscriber station* (*SS). Base station (BS)* selalu menyiapkan *authorization key (AK)* ke *subscriber station* (*SS)* atas suatu permintaan. *Base station (BS)* akan mendukung dua aktivitas *authorization key (AK)* untuk setiap *client subscriber station* (*SS). Authorization key (AK)* mempunyai batas *lifetime* dan secara periodik akan di-*refresh*.

2.7.4. Privasi Data

Untuk menjaga privasi data pada sistem mobile WiMax ini digunakan metode enkripsi Adavnce Encryption Standard (AES). Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi *bytes,* yaitu :

1. *SubBytes*, transformasi byte dimana setiap elemen pada state akan dipetakan dengan menggunakan sebuah tabel substitusi (*S-Box*).
2. *ShiftRows,* Transformasi Shiftrows pada dasarnya adalah proses pergeseran bit dimana bit paling kiri akan dipindahkan menjadi bit paling kanan (rotasi bit).
3. *Mixcolumns,* Mixolumns mengoperasikan setiap elemen yang berada dalam satu kolom pada *state*. Elemen pada kolom dikalikan dengan suatu polinomial tetap $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$.
4. A*ddRoundKey,* Pada proses AddRoundKey, sebuah *round key* ditambahkan pada *state* dengan operasi bitwise XOR. Setiap *round key* terdiri dari *Nb word* dimana tiap *word* tersebut akan dijumlahkan dengan *word* atau kolom yang bersesuaian dari *state.*

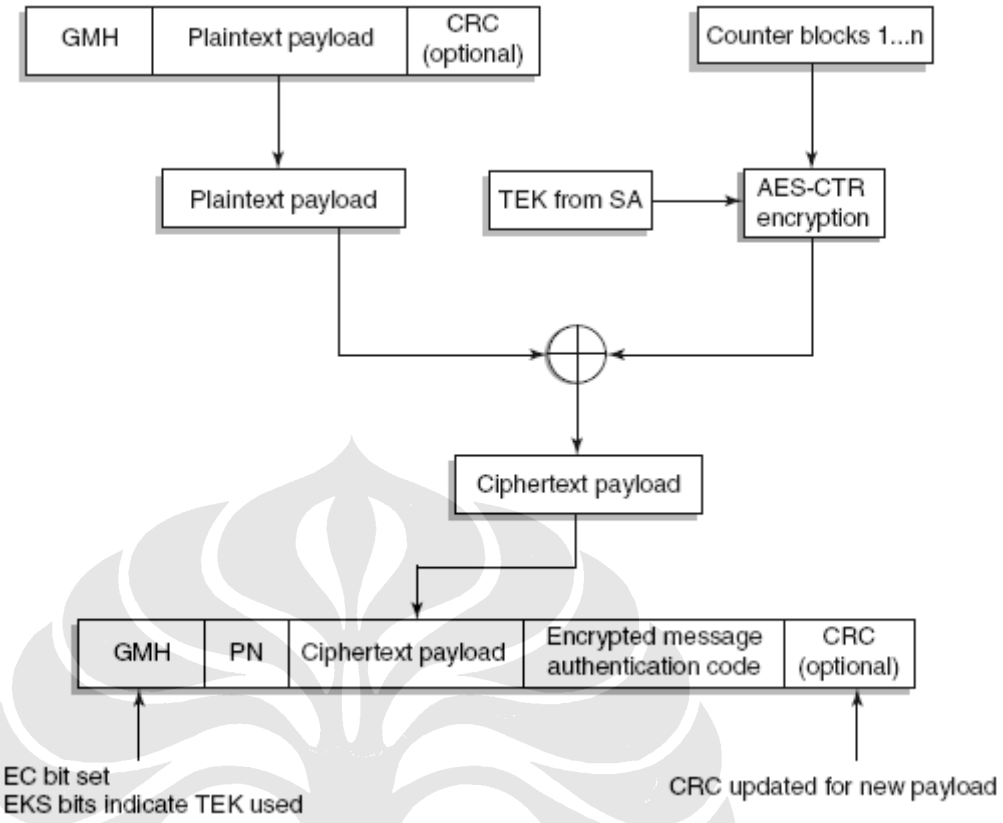
Pada awal proses enkripsi, *input* yang telah dikopikan ke dalam *state* akan mengalami transformasi byte *AddRoundKey*. Setelah itu, *state* akan mengalami transformasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulang-ulang sebanyak *Nr*. Proses ini dalam algoritma AES disebut sebagai *round function*. *Round* yang terakhir agak berbeda dengan *round-round* sebelumnya dimana pada *round* terakhir, *state* tidak mengalami transformasi *MixColumns.*

Transformasi *cipher* dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan *inverse cipher* yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers *cipher* adalah:

1. *InvShiftRows,* yaitu transformasi byte yang berkebalikan dengan transformasi *ShiftRows*. Pada transformasi *InvShiftRows,* dilakukan pergeseran bit ke kanan sedangkan pada *ShiftRows* dilakukan pergeseran bit ke kiri.
2. *InvSubBytes,* yaitu merupakan transformasi *bytes* yang berkebalikan dengan transformasi SubBytes. Pada *InvSubBytes*, tiap elemen pada *state* dipetakan dengan menggunakan tabel *inverse S-Box*
3. Pada *InvMixColumns*, kolom-kolom pada tiap *state* (*word*) akan dipandang sebagai polinom atas GF(2^8) dan mengalikan modulo $x^4 + 1$ dengan polinom tetap $a^{-1}(x)$ yang diperoleh dari :

   $$a^{-1}(x) = \{0B\}x^3 + \{0D\}x^2 + \{09\}x + \{0E\}.$$

4. *AddRoundKey* Transformasi *Inverse AddRoundKey* tidak mempunyai perbedaan dengan transformasi *AddRoundKey* karena pada transformasi ini hanya dilakukan operasi penambahan sederhana dengan menggunakan operasi bitwise XOR.[5]



Gambar 2.15 Diagram Blok Pengenkripsian Payload

BAB 3

PERANCANGAN SISTEM

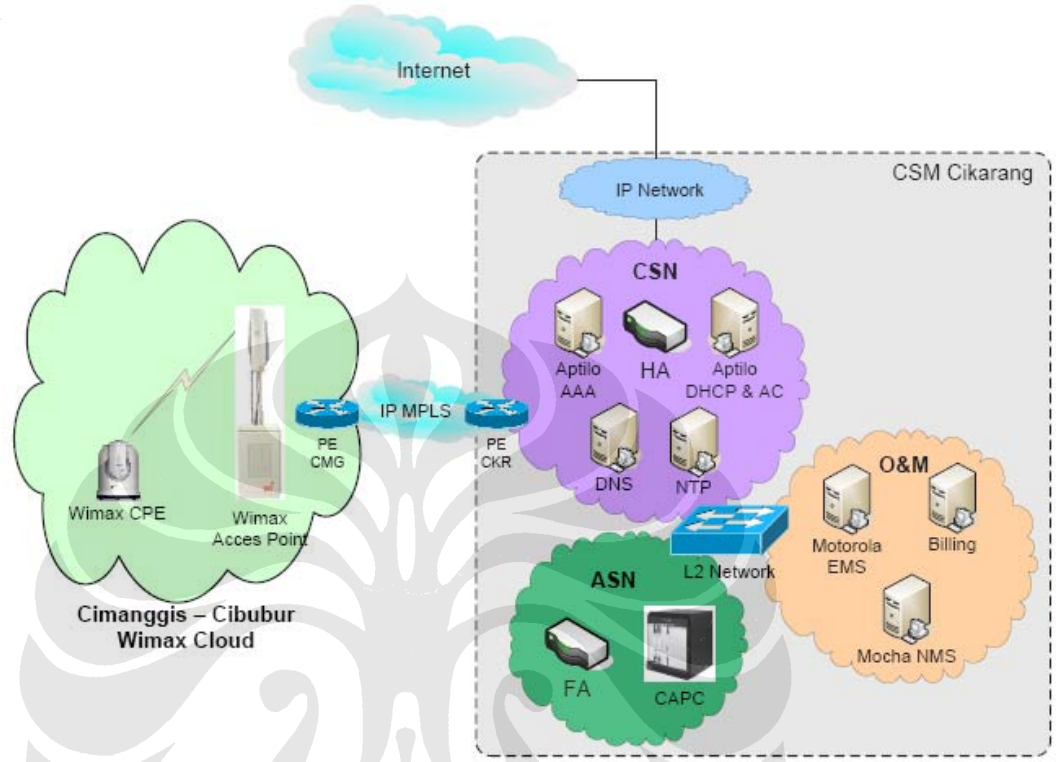
3.1. Deskripsi Umum Sistem

Dalam skripsi ini digunakan sistem WiMax yang telah di implementasikan dan sedang diujicobakan di PT. Citra Sari Makmur. Seperti halnya pada sistem WiMax pada umumnya, disini terdiri atas *subscriber station* (SS), *base station* (BS) atau akses poin WiMax serta sistem jaringan. Dalam sistem ini, PT. Citra Sari Makmur sebenarnya memiliki 2 *base station*, yaitu di stasiun Cimanggis dan stasiun Cikarang.

Sedangkan sistem jaringan yang digunakan pada sistem ini semuanya berada di stasiun Cikarang. Sistem tersebut terdiri atas *Acces Service Network* (ASN), *Connectivity Service Network* (CSN) dan *Opreation and Monitoring* (O&M). ASN adalah sub-sistem yang berperan dalam menyediakan layanan akses radio bagi stasiun pelanggan. ASN mengatur hubungan fisik antara stasiun pengguna dengan akses poin melalui sinyal radio. Melalui ASN inilah sistem WiMax mengatur sinyal carrier yang dipancarkan oleh akses poin kepada stasiun pelanggan. Sub sistem ASN ini terdiri atas perangkat *Carrier Acces Point Controller* (CAPC) dan *Foreign Agent* (FA).

Untuk mengatur konektivitas IP terhadap stasiun pelanggan, pada sistem WiMax ini diatur oleh sub sistem CSN. Apabila ASN telah memberikan sambungan secara fisik melalui radio pada stasiun pelanggan, maka kemudian layanan hubungan dan pertukaran data berikutnya ditangani oleh CSN. Sub sistem CSN ini terdiri atas beberapa perangkat yang bekerja pada protokol IP.Perangkat yang pertama adalah server AAA (autentikasi, autorisasi dan akunting). Pada server AAA inilah sebagian besar sistem keamanan ditangani. Perangkat tersebut berperan dalam proses autentikasi, autorisasi serta pengaturan akun pengguna. Selain itu terdapat pula server DHCP yang mengatur pemberian alamat IP pada stasiun penguna dan sistem yang terkait, server *Domain Name System* (DNS) serta server *Network Time Protocol* yang mengatur sistem sinkronisasi dan pewaktuan.

Tiap-tiap sub sistem tersebut dihubungkan melalui jaringan L2 yang ada pada stasiun Cikarang. Sedangkan Stasiun Cimanggis dihubungkan melalui jaringan IP MPLS.



Gambar 3.1 Diagram Jaringan WiMax

3.2. Perangkat Yang Digunakan

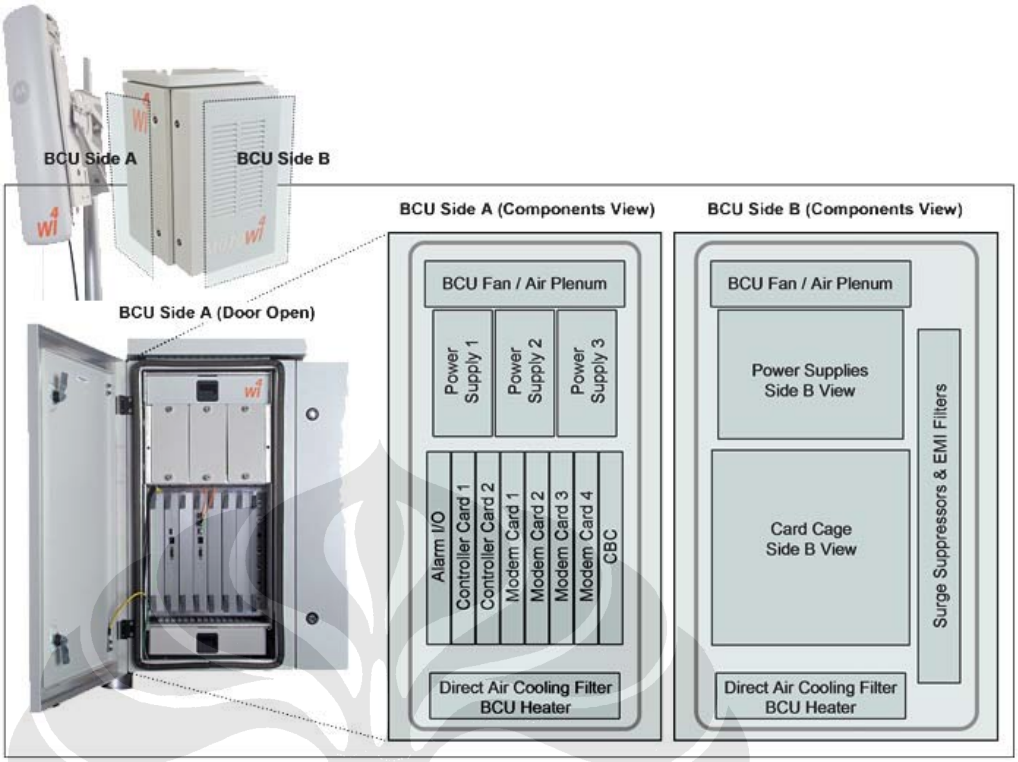
Perangkat yang digunakan pada sistem ini adalah sesuai dengan perangkat yang ada pada PT. Citra Sari Makmur. Perangkat tersebut antara lain :

3.2.1. Stasiun Utama

Untuk perangkat *base station* dalam sistem ini digunakan *Motorolla MotoWi4 Wimax Acces Point*. Perangkat akses poin WiMax ini berfungsi untuk menangani semua stasiun pelanggan yang berada dalam jangkauannya. Saat ini terdapat dua stasiun utama dan daerah yang terjangkau adalah daerah Cimanggis dan Cikarang. Perangkat tersebut mendukung spesifikasi sebagai berikut :

Tabel 3.1 Daftar Spesifikasi Perangkat Akses Poin WiMax

Modul Diversiti RF	
Arsitektur	Dual Antenna Elements Dual TX / Rx Chains MIMO dengan Adaptive Beam Forming
Dimensi	712H x 178W x 229D mm (28”x7”x9”)
Berat	16 kg* (35 lbs)
Base Control Unit	
Arsitektur	Weatherized Outdoor Unit Pole atau Ground Mounted Mobilitas penuh Carrier-Class Availability
Dimensi	788H x 508W x 483D mm (31”x20”x19”)
Berat	68 kg (150 lbs)
Stasiun Pelanggan	
» 3000 pengguna dengan kombinasi aktif, idle & sleep » 256 pengguna aktif per sektor » 256x4=1024 pengguna aktif untuk 4 sektor	
Aplikasi	
» Fixed, nomadic dan mobile » Data services and carrier-class voice » Multimodal handsets » MIMO	



Gambar 3.2 Perangkat Base Station WiMax

3.2.2. Stasiun Pelanggan

Sedangkan untuk perangkat stasiun pelanggan, dalam system ini digunakan Motorolla CPE i300 *Series*. Perangkat tersebut mendukung spesifikasi sebagai berikut :

Tabel 3.2 Daftar spesifikasi perangkat CPE

Radio Performance	500 mW output power Highly sensitive receiver Sectorized antenna array – orientation independent performance Convolution Turbo Coding (CTC) Hybrid Automatic Repeat request (HARQ)
Konektivitas	1 Port Ethernet 2 Ports ATA terintegrasi (VoIP)
Certification	WiMAX Forum Certification Wave 1 7 MHz and 5 MHz Channel for 3.5 GHz 5 MHz and 10 MHz Channel for 2.5 GHz and 2.3 GHz

Quality of Service Classes	BE (Best Effort) UGS (Unsolicited Grant Service) RTPS (Real Time Polling Service) NRTPS (Non Real Time Polling Service) ERTPS (Extended Real Time Polling Service)
Security	Device authentication based on X.509 digital certification Authentication methods according to IEEE 802.16e, EAP-TLS and also EAP-TTLS AES (128-bit) Data Encryption and Authentication
Remote Configuration and Software Upgrade	OTA (Over The Air) field upgradeable SNMP v3 Agent
OS Compatibility	Windows / Mac
RF Performance	Sensitivity: >5dB better than WiMAX Forum Specifications Antenna Gain: >7dBi TX power out: +27dBm (0.5 Watts) Noise Figure: 5 dB
Mechanical and Electrical	External Power: 100-250 Volts AC input Operating Temp: 0°C to 40°C Operating Humidity: 5% to 95%, non-condensing US and International plug support

Piranti CPE yang berfungsi sebagai terminal yang menghubungkan pelanggan ke stasiun utama ini memiliki beberapa tipe. Dua tipe yang digunakan dalam sistem ini antara lain adalah tipe wolverine dan tipe badger.

Gambar 3.3 CPE Motorolla tipe wolverine

CPE tipe wolverine ini cenderung digunakan untuk kebutuhan terminal bergerak. Sedangkan tipe badger lebih cenderung untuk digunakan pada kondisi diam dalam ruangan.

Gambar 3.4 CPE Motorolla tipe badger

3.3. Metode Sistem Keamanan yang Digunakan

Pada sistem WiMax yang digunakan di PT. Citra sari Makmur ini, menggunakan mode sistem pengamanan, antara lain :

- Sertifikasi digital X.509
- Protokol autentikasi EAP-TTLS (*Extensible Authentication Protocol Tunneled Transport Layer Security*).
- Enkripsi *Advance Encryption Standard* (AES) 128-bit

3.4. Program Simulasi Sistem Keamanan

Pada penulisan skripsi ini juga dilakukan simulasi proses pengamanan data pada Mobile WiMax. Simlulasi tersebut menunjukkan proses-proses seperti : inisialisasi, autorisasi, autentikasi dan enkripsi data dengan menggunakan metode AES-128 bit. Simulasi dengan program tersebut digunakan untuk membantu memahami tahapan-tahapan proses pengamanan yang terjadi terutama proses enkripsi data dengan menggunakan metode AES-128 bit.

Pada perancangan perangkat lunak simulasi ini diasumsikan terdapat dua pihak, yaitu SS dan BS dimana akan dilakukakn koneksi dan pertukaran data

antara kedua pihak tersebut. Simulasi ini dimulai dengan SS mengirimkan sinyal permintaan inisiasi dengan menyertakan data identitas dan kredensial yang dimilikinya. Kemudian disisi BS melakukan pemeriksaan dan autentikasi terhadap data yang dikirimkan SS tersebut untuk kemudian mengirimkan autorisasi pada SS bersangkutan. Kemudian baru dilakukan transfer data yang dienkripsi dengan menggunakan metode AES-128 bit.

Pada simulasi ini kunci yang digunakan enkripsi data dikirimkan dari sisi BS dengan kunci acak yang dibangkitkan oleh library yang terdapa pada program Python.

Dalam perangkat lunak simulasi ini akan ditampilkan data sumber yang akan dikirim kemudian data chiper yang sudah terenkripsi dan data yang telah sampai ditujuan dengan didekripsi. Sehingga bisa dibandingkan masing-masing data tersebut.

3.4.1. Platform Perangkat Lunak Simulasi

Perangkat lunak simulasi ini dikembangkan dengan menggunakan platform antara lain sebagai berikut :

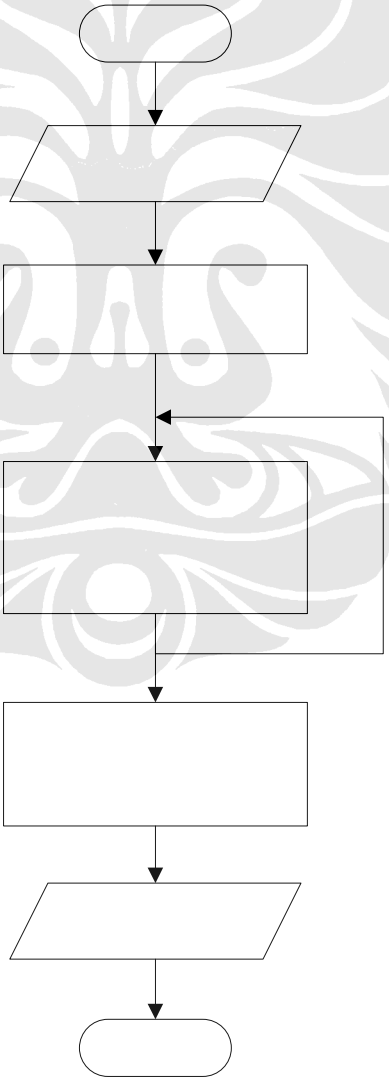
- Ubuntu 8.10 intrepid-ibex kernel 2.6.27-7
- Python 2.5.2
- GCC 4.3.2
- WxPhyton 2.8.8.0
- WxGlade 0.6.3

3.4.2. Diagram Alir Perangkat Lunak Simulasi

Berikut ini adalah diagram alir yang digunakan dalam perancangan perangkat lunak simulasi sistem keamanan untuk Mobile WiMax ini :

3.4.2.1. Diagram Alir Enkripsi

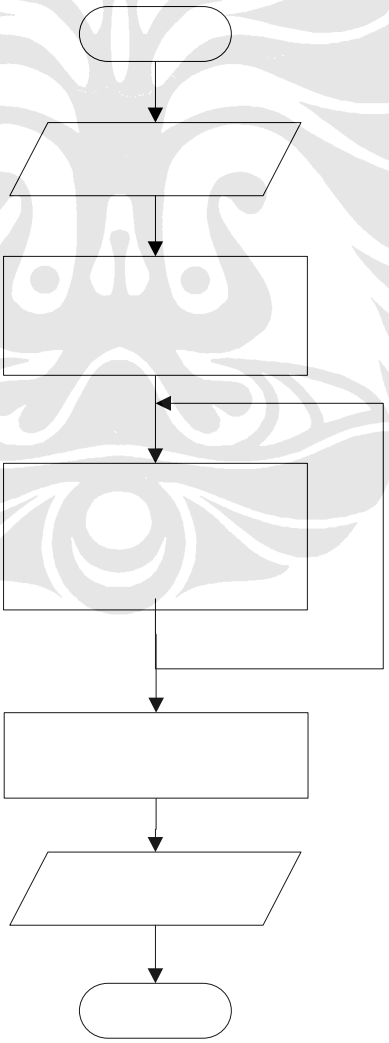
Proses enkripsi dimulai dengan mengambil masukan berupa data informasi. Data informasi tersebut kemudian diproses dalam bentuk blok bit. Kemudian dilakukan proses "*AddRoundKey*", yaitu proses dimana sebuah *round key* ditambahkan dengan operasi bitwise XOR. Setelah itu kemudian dilakukan proses "*SubBytes*", "*ShiftRows*", "*MixCollumns*" dan "*AddRound Key*". Proses tersebut dilakukan berulang-ulang sebanyak jumlah *round* dikurangi satu (Nr-1). Kemudian dilakukan sekali lagi, tetapi tanpa proses "*MixCollumns*". Maka. dari proses-proses tersebut didapatkan data berupa *chiper text* atau data yang sudah terenkripsi.



Gambar 3.5 Diagram Alir Enkripsi

3.4.2.2. Diagram Alir Dekripsi

Proses dekripsi, gambaran umumnya merupakan proses kebalikan dari proses enkripsi. Proses ini dimulai dengan mengambil data masukan berupa *chiper text* atau data yang sudah terenkripsi. Kemudian pada bit-bit data itu dilakukan proses-proses inverse dari proses enkripsi. Yang pertama yaitu "*AddRoundKey*", "*InvShiftRows*" dan "*InvSubBytes*". Proses tersebut kemudian dilanjutkan dengan proses yang sama namun ditambah dengan proses "*InvMixCollumns*" terlebih dahulu setelah proses "*AddRoundKey*". Sama halnya pada proses enkripsi, proses ini juga dilakukan berulang-kali sebanyak jumlah *round* dikurangi satu (Nr-1). Proses berikutnya adalah dilakukan "*AddRoundKey*" kembali. Maka. dari proses-proses tersebut didapatkan kembali data berupa data informasi seperti semula.



Gambar 3.6 Diagram Alir Enkripsi

BAB 4

ANALISIS DAN PENGUJIAN SISTEM

4.1. Hasil Pengujian dan Analisis Sistem

4.1.1. Pengujian dan Analisis Pemindaian Frekuensi

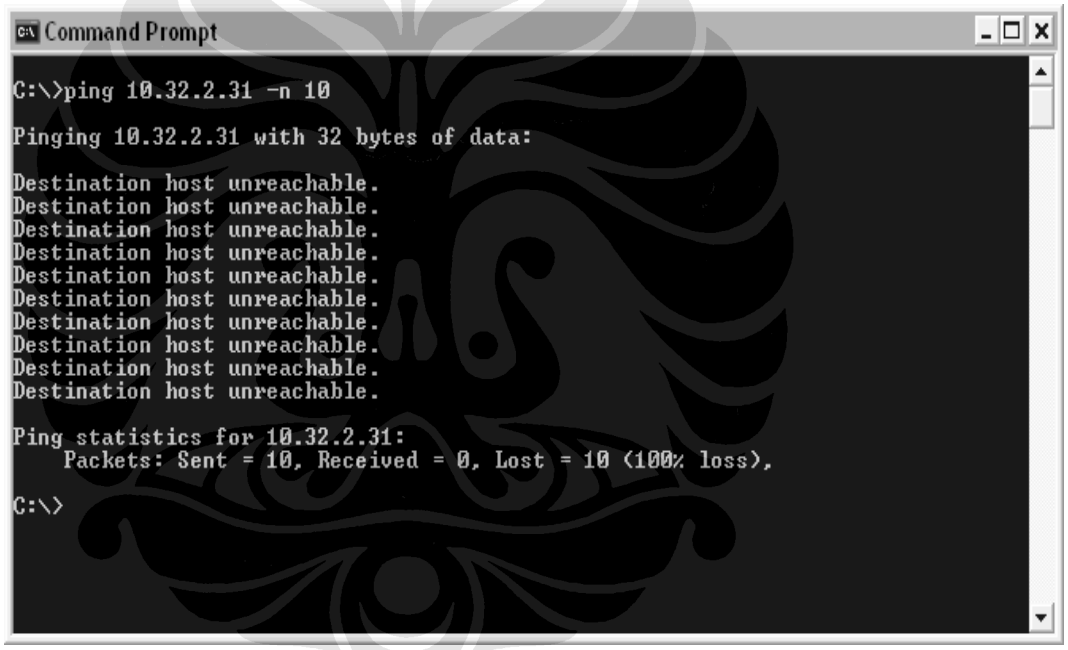
Pengujian pertama yang dilakukan adalah pengujian pemindaian akses poin WiMax. Sebelum melakukan koneksi tiap SS melakukan pemindaian frekuensi-frekuensi sesuai dengan yang yang telah dikonfigurasi pada terminal CPE yang digunakan. Apabila terdapat akses poin WiMax terletak dalam jangkauannya,maka terminal pengguna tersebut otomatis akan mengenalinya. Pada pengujian kali ini perangkat CPE dan akses poin WiMax menggunakan frekuensi 2,5 GHz.

Gambar 4.1 Pemindaian Akses Poin WiMax yang Tersedia

Dari Gambar 4.1 dapat dilihat bahwa stasiun pengguna mendeteksi hanya ada satu akses poin WiMax yang tersedia pada jangkauannya. Pada mode seperti

ini stasiun pengguna tersebut sbenarnya secara fisik sudah mendapatkan sinyal dari akses poin WiMax tersebut, namun koneksinya belum terbentuk dan tidak dapat melakukan transfer data. Hal ini bisa dilihat dari nilai RSSI-nya yang sebesar -25 dBm dan CINR-nya sebesar 28 dB.

Untuk membentuk koneksi, stasiun pengguna tersebut harus melakukan inisiasi dimana ia mengirimkan permintaan koneksi dengan menyertakan data identitas terminal dan kredensial yang disertakannya untuk di autentikasi oleh stasiun utama. Karena belum terkoneksi, maka stasiun pengguna tersebut belum dapat melakukan transfer data apapun. Hal ini bisa dilihat dari hasil tes ping ke server EMS yang berada pada stasiun utama.

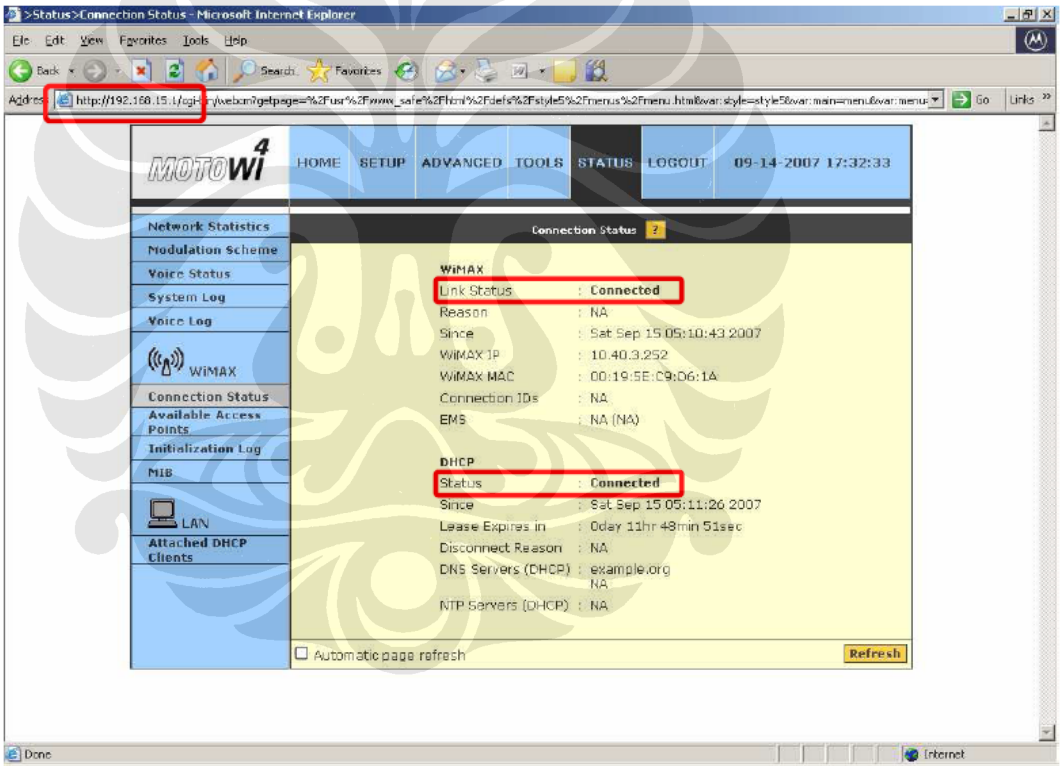


Gambar 4.2 Hasil Tes Ping dari CPE ke EMS Pada Saat CPE Belum Melakukan Inisiasi

4.1.2. Pengujian dan Analisis Autorisasi

Apabila Stasiun pengguna berada dalam jangkauan akses poin WiMax dan akses poin tersebut pada status tersedia oleh stasiun pengguna, maka stasiun pengguna tersebut bisa melakukan inisiasi untuk memulai koneksi dengan stasiun utama. Pada saat melakukan inisiasi, stasiun pengguna mengirimkan sinyal permintaan dan menyertakan data-data identitas terminal pengguna untuk di autentikasi oleh stasiun utama.

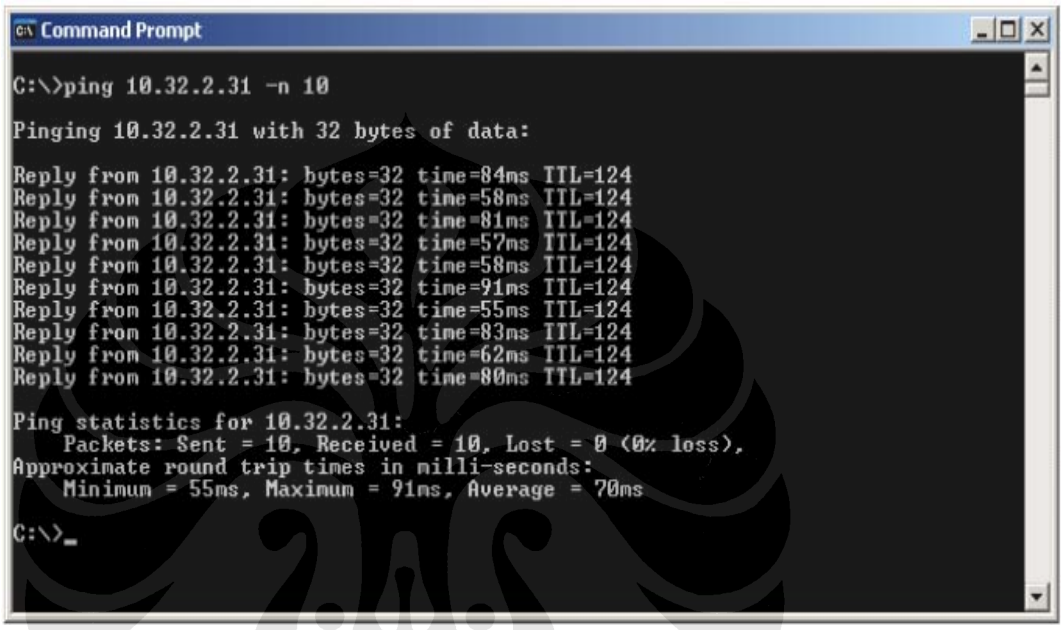
Sertifikat digital yang dikirimkan tersebut akan diteruskan ke server autentikasi. Apabila sertifikat digital itu dikenali sebagai pengguna yang berhak mendapatkan koneksi dari stasiun utama, maka server autentikasi akan memberikan informasi ke stasiun utama untuk memberikan balasan denga mengautorisasi dan mengirimkan CID untuk membentuk sesi-sesi koneksi berikutnya. Bila server autentikasi menolak proses autentikasi karena sertifikasi kredensial yang dikirimkan menunjukkan bahwa stasiun pengguna tidak berhak mendapatkan koneksi dari stasiun utama, maka stasiun utama kan menginformasikan pada CAPC agar stasiun pengguna tersebut diberikan null point oleh *adaptive beamforming antenna*.



Gambar 4.3 Hasil Pengujian Status Autentikasi Terminal Pengguna WiMax

Setelah terminal pengguna membentuk sesi dengan stasiun utama, berikutnya stasiun utama akan memberikan alamat IP pada terminal pengguna melalui server DHCP. Dalam sistem ini alamat IP salalu diberikan oleh stasiun utama secara dinamis.

Hal ini ditunjukkan Gambar 4.3 yang menunjukkan status link dan DHCP yang telah tersambung dengan menampilkan status "*link connected*" dan "*DHCP connetced*". Pada Gambar 4.3 itu juga ditunjukkan alamat IP yang ditentukan oleh server DHCP stasiun utama adalah 10.40.3.252. Selain itu alamat mac dari terminal tersebut juga dikenali, yaitu 00:19:5E:C9:D6:1A.



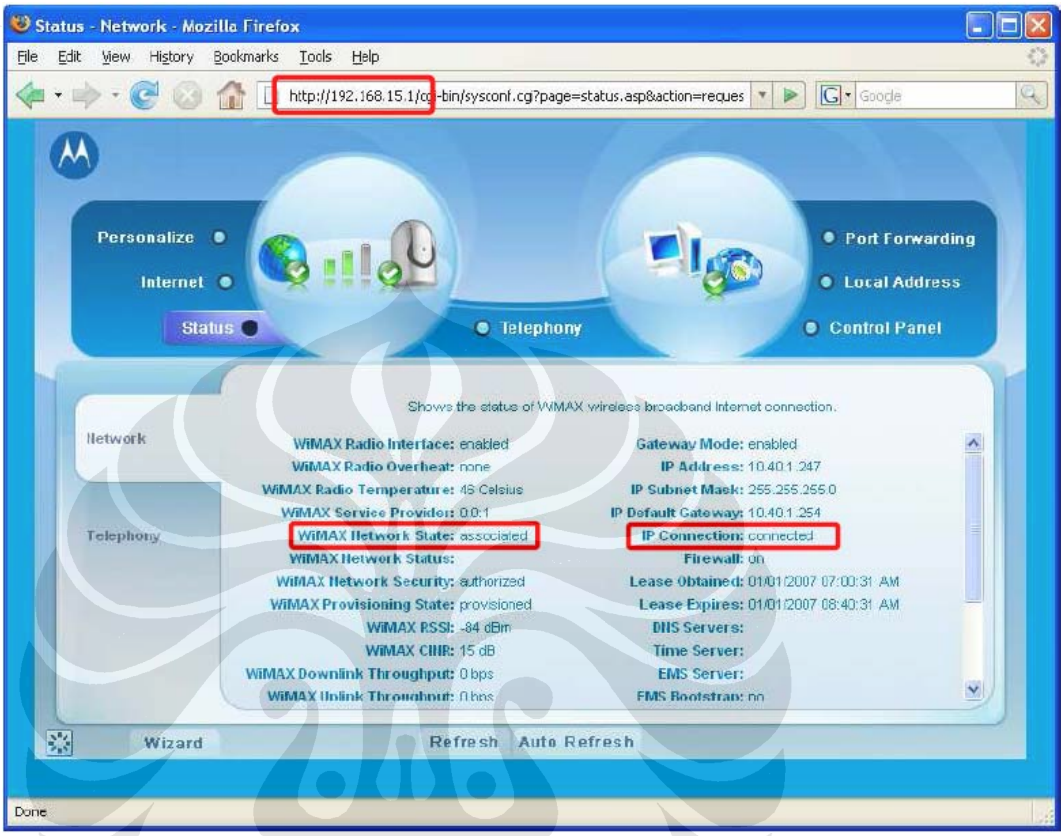
Gambar 4.4 Hasil Tes Ping Dari CPE ke Server EMS Pada Saat Status Tersambung

Sesi yang dibentuk antara stasiun utama dengan stasiun pengguna terus diperbarui dengan terus mengirimkan CID tiap mengirimkan data dan memperbarui kunci yang digunakan sebagai proses proteksi dengan enkripsi. Ketersambungan terminal pengguna ini bisa dibuktikan dengan hasil tes ping dari arah CPE dengan alamat IP 10.40.3.252 menuju server EMS dengan alamat IP 10.32.2.31. Dari semua paket ICMP yang dikirimkan lewat tes ping tersebut, 100% sukses dengan latensi maksimum 91 ms.

4.1.3. Pengujian dan Analisis Transfer Data FTP

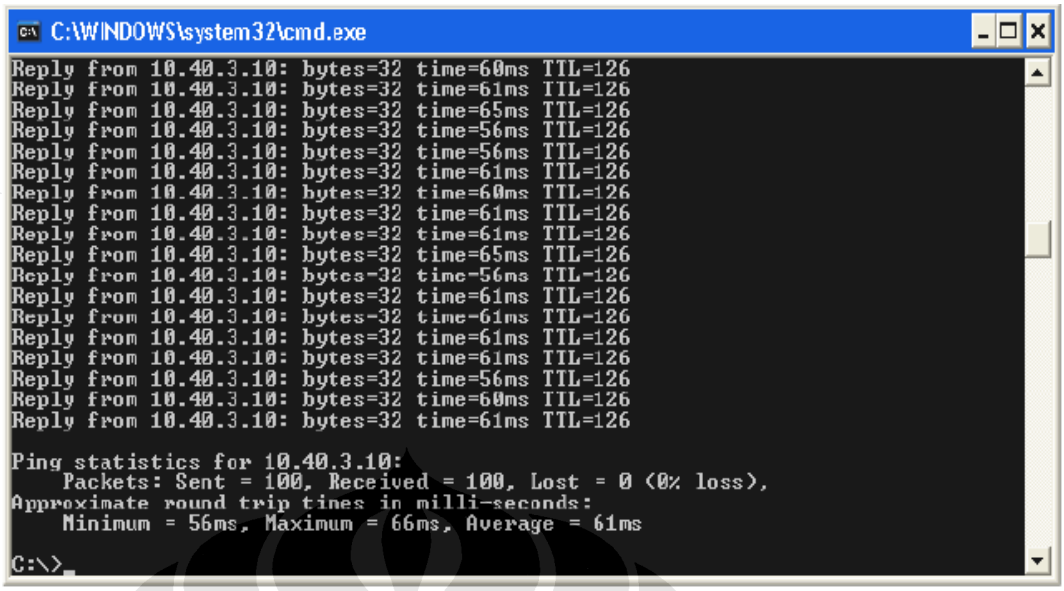
Pengujian beerikutnya adalah dengan melakukan transfer data melalui jaringan WiMax yang telah tersambung. Transfer data tersebut akan dilakukan

antara CPE dengan server FTP yang memiliki IP 10.40.3.10. Pengujian FTP ini dilakukan secara dua arah, yaitu FTP unduh dan FTP unggah.



Gambar 4.5 Status Koneksi Sebelum Melakukan FTP

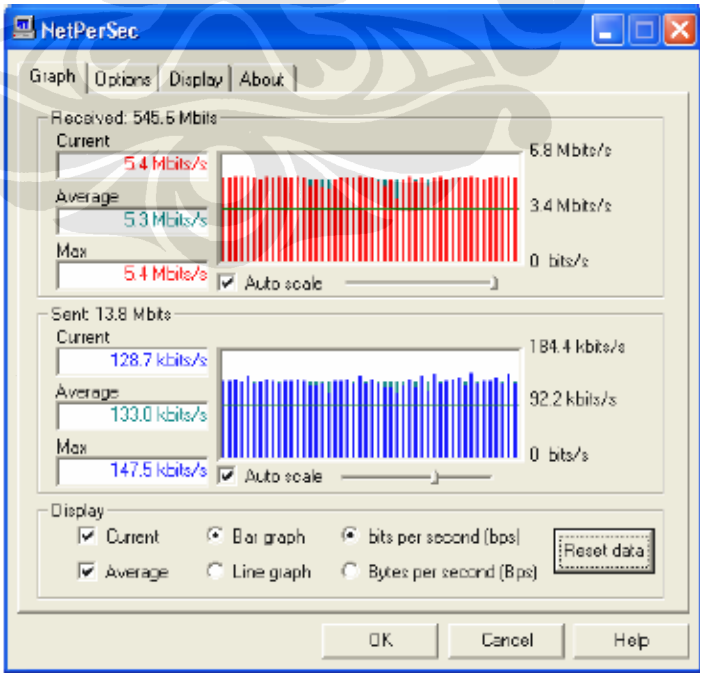
Sebelum melakukan pengujian transfer data melalui FTP, terlebih dulu perlu dilakukan pengujian koneksi dari CPE tersebut ke server FTP. Yaitu dengan melakukan tes ping dari CPE ke server FTP.



Gambar 4.6 Hasil Tes Ping Dari CPE ke Server FTP

4.1.3.1. Pengujian Transfer Data FTP Downlink

Pengujian transfer data FTP downlink dilakukan dengan mengambil file dari server FTP oleh terminal pengguna. Dengan mengambil file yang cukup besar maka akan terjadi transfer data secara terus menerus dan membutuhkan sesi koneksi yang berkesinambungan.



Gambar 4.7 Trafik Saat Pengujian FTP Downlink

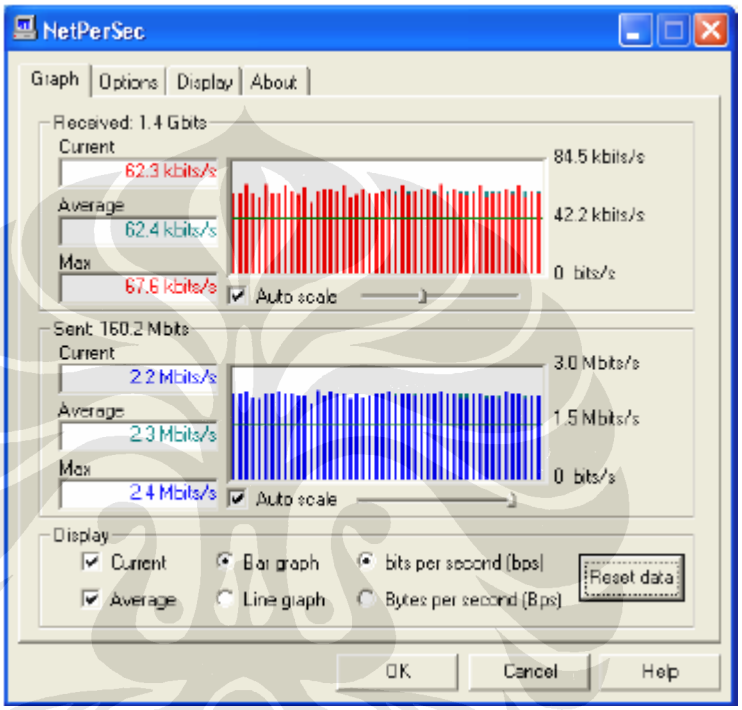
Pada saat melakukan transfer data melalui FTP dapat diamati pada status MAC yang ada pada terminal CPE. Dari Gambar 4.8 dapat dilihat bahwa pada saat itu jumlah paket yang masuk (DL) ke CPE adalah 2738 sedangkan yang keluar (UL) adalah 15. Hal ini karena proses yang sedang terjadi adalah proses unduh, sehingga trafik lebih banyak ke arah CPE. Sedangkan untuk trafik keluar (UL), meskipun tidak ada aktivitas unggah masih terdapat trafik keluar (UL). Hal ini karena meskipun tidak dilakukan aktivitas unggah, CPE akan terus mengirimkan data-data yang besarnya kecil yang berupa kredensial dan CID untuk tetap membentuk sesi antara CPE dengan stasiun utama. Selain itu juga terdapat trafik SNMP antara CPE dengan server manajemen EMS.

Gambar 4.8 Status MAC Pada CPE Saat Melakukan FTP

Selain itu pada Gambar 4.8 juga ditunjukkan status dari berbagai parameter PKM. Di Gambar 4.8 tersebut juga ditunjukkan bahwa "*AK Life Time*" adalah 17277849. Angka ini menunjukkan waktu sisa ata panjang usia dari kunci publik yang digunakan bersama antara stasiun utama dengan terminal pengguna. Kunci tersebut akan terus diperbarui untuk tetap membentuk koneksi.

4.1.3.2. Pengujian Transfer Data FTP Uplink

Selain pengujian transfer data downlink juga dilakukan pengujian transfer data uplink. Hal ini sama saja dengan proses FTP downlink hanya saja trafiknya terbalik. Pada proses ini trafik Keluar (UL) CPE lebih tinggi dibandingkan trafik masuk (DL) ke CPE.



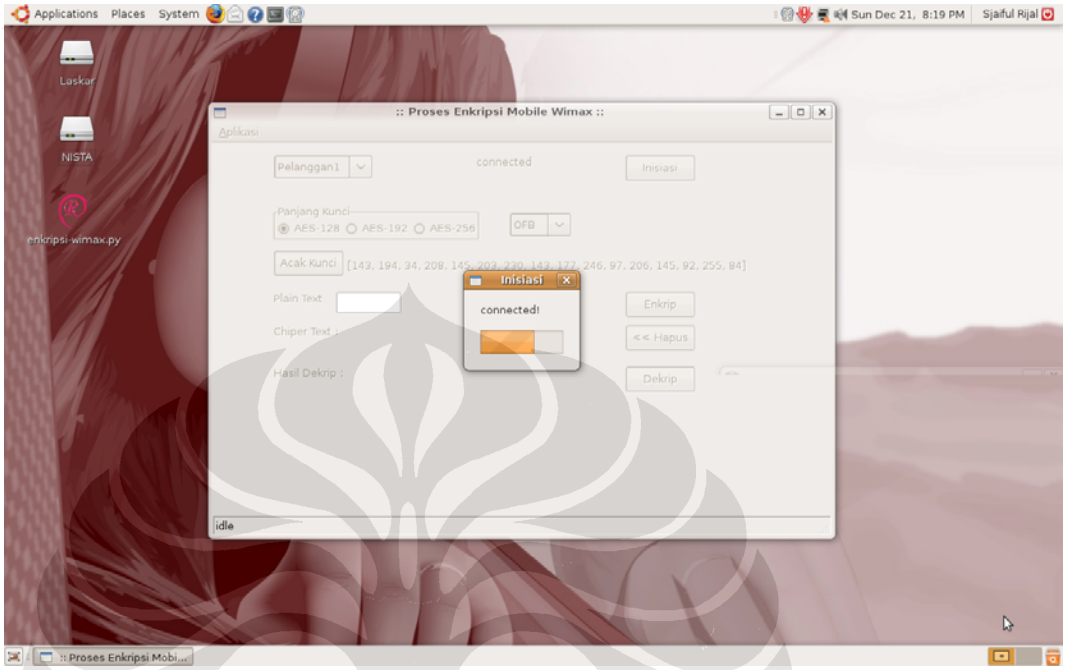
Gambar 4.9 Trafik Saat Transfer Data FTP Uplink

Pada proses transfer data FTP Uplink ini trafik yang keluar (UL) tidak sebesar trafik masuk (DL) pada saat transfer data FTP downlink. Hal ini terjadi karena layanan yang diberikan memang asimetris. Yaitu kapasitas downstream lebih tinggi daripada upstream.

4.2. Hasil Pengujian dan Analisis Simulasi

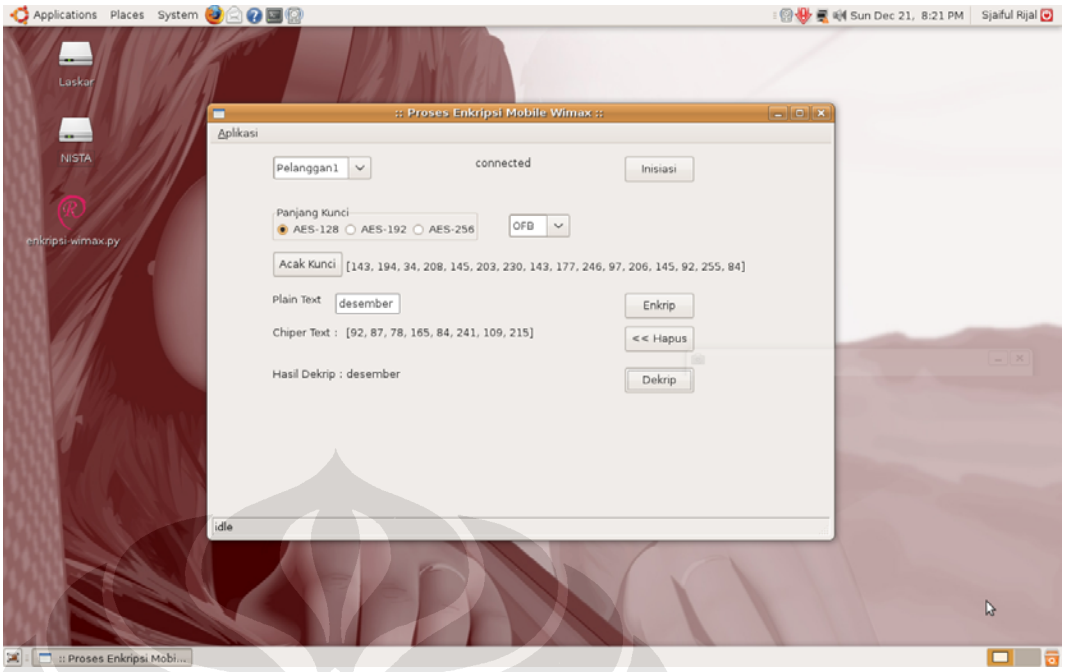
Untuk mengetahui proses pengamanan data pada sistem Mobile WiMax, digunakan perangkat lunak untuk mensimulasikannya. Pada program simulasi ini dilakukan proses pengamanan data dengan cara enkripsi dan dekripsi. Data dienkripsi dengan menggunakan metode *Advance Encryption System* (AES) 128

bit. Dari Gambar 4.10 dapat dilihat hasil eksekusi program shell linux melalui program python2.5.



Gambar 4.10 Tampilan Program Simulasi Proses Inisiasi

Pada simulasi tersebut ditunjukkan proses inisiasi SS terhadap BS. Dalam program tersebut diasumsikan terdapat 4 SS pelanggan, dimana masing-masing memiliki kredensialnya sendiri. Dari tampilan program pada Gambar 4.10 tampak SS Pelanggan1 melakukan permintaan sambungan pada BS. Pada proses ini, SS mengirimkan data kredensialnya berupa MAC dan sertifikasi digital berbasis X.509 yang dimiliki. Kamudian BS memeriksanya, untuk menyamakan dengan data yang dimiliki oleh BS. Bila cocok, maka seperti pada tampilan program yang ada di Gambar 4.10, maka BS akan memberikan koneksi pada SS Pelanggan1 tersebut.



Gambar 4.11 Tampilan Program Simulasi Proses Enkripsi

Setelah proses inisiasi, program simulasi ini dapat menjalankan simulasi proses enkripsi, dimana terdapat tiga pilihan panjang kunci yang akan digunakan pada metode enkripsi AES. Mode-mode enkripsi berdasarkan panjang kuci tersebut, antara lain : AES-128, AES-192 dan AES-256. Karena pada sistem Mobile WiMax yang sedang diuji coba menggunakan metode enkripsi AES dengan panjang kunci 128 bit, maka digunakan AES-128.

Pada Gambar 4.11, ditampilkan kunci-kunci yang digunakan pada proses enkripsi-dekripsi ini. Kunci-kunci tersebut dibangkitkan secara acak yang kemudian akan didistribusikan ke SS. Pada program simulasi ini diasumsikan pengiriman *plaintext* dengan informasi berisi “desember”. Dengan 128 bit kunci AES yang dibangkitkan secara acak (143,194, 34, 208, 145, 203, 143, 177, 246, 97, 206, 145, 92, 255, 84) dihasilkan kode *chipertext* (92,87,78,165, 84, 241, 109, 215).

Angka-angka tersebut merupakan bentuk integer dari tiap blok 8 bit dari masing-masing kode.Enkripsi ini dilakukan dalam bentuk bit namun dilakukan per blok.

Dalam bentuk chipertext tersebutlah dilakukan pengiriman data, sehingga data informasi dapat terjamin kerahasiaannya. Karena hanya dengan kunci yang sama, informasi tersebut dapat terbaca seperti semula.

BAB 5

KESIMPULAN

Dari hasil pengujian dan analisis sistem WiMax di PT. Citra Sari Makmur serta melaui simulasi yang telah dilakukan, maka dapat diambil beberapa kesimpulan sebagai berikut :

1. Suatu terminal pelanggan meskipun dalam jangkauan dan mendeteksi keberadaan akses poin WiMax tidak akan dapat terkoneksi jika tidak melakukan inisiasi.
2. Untuk mengamankan data yang ditransfer, sistem mobile WiMax ini menggunakan kunci publik yang dibangkitkan BS dengan lifetime tertentu dan kemudian diperbarui secara terus menerus.
3. Sistem Mobile WiMax menggunakan alamat IP dinamis yang ditentukan oleh server DHCP.
4. Sistem Mobile WiMax menggunakan metode enkripsi *Advance Encryption Standard* (AES)128 dalam melindungi informasi yang ditransfer antara BS dan SS.
5. Sertifikat digital X.509 digunakan oleh sistem mobile WiMax untuk mengidentifikasi dan mengautentikasi pengguna-pengguna yang akan menggunakan layanan pada BS.
6. Server Autentikasi bersinergi dengan CAPC untuk memberikan layanan secara optimal pada pengguna yang berhak dan mencegah penggunaan layanan tanpa hak.

DAFTAR REFERENSI

[1] Ahson, Syed & Ilyas, Mohammad, *Wimax Standard and Security*, (CRC Press, 2008) hal 199-203, 210-213, 231

[2] Yang Xiao, *WiMax/MobileFi Advanced Reasearch and Technology*, (Auerbach Publications, 2008) hal 108-110.

[3] Wongthavarawat, Kitti, *IEEE 802.16 WiMax Security*, (Thai Computer Emergency Response Team National Electronics and Computer Technology Center, Thailand, 2005)

[4] Sutton, Rorer, *Secure Communications Applications and Management*, (John Wiley & Sons Ltd, 2002) hal 34.

[5] Federal Information Processing Standard, *Advance Encryption Standard*, (National Institute of Standard and Technology, Amerika Serikat, 2001)

DAFTAR PUSTAKA

Siyamta, "Sistem Keamanan Pada WorldwideInteroperability for Microwave Access", Ilmu Komputer, 2005.

Raharjo, Budi, "Pengantar Kriptografi", Indocisc, 2005

Suprapti, Swanti, "Studi Keamanan Data Dengan Metode Public Key Cryptography", Institut Teknologi Bandung, 2003.

Sukaridhoto, Sritrusta, dkk, "Teknik keamanan Keamanan pada VoIP dengan Virtual Private Networking dan Kriptografi Serta Korelasi Terhadap Bandwidth dan Intelligibility Suara", EEPIS-ITS, 2006.

Raharjo, Budi, "Keamanan Sistem Informasi Berbasis Internet", PT. Insan Infonesia & Indocisc, 2005

Gunawan Wibisono & Gunadi Dwi Hartono, " Mobile Broadband, Tren Teknologi Wireless Saat Ini dan Masa Datang", Informatika, 2008.

Noprianto, "Phyton dan Pemrograman Linux", ANDI Jogakarta, 2002

Thomas, Tom, "Network Security First-Step", Cisco Press, 2004