

Sistem Keamanan Pada *Worldwide Interoperability for Microwave Access (WiMAX)*

Siyamta
must_yamta@yahoo.com

Lisensi Dokumen:

Copyright © 2005 IlmuKomputer.Com

Seluruh dokumen di **IlmuKomputer.Com** dapat digunakan, dimodifikasi dan disebarakan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari **IlmuKomputer.Com**.

ABSTRAK

Standar 802.16 dikembangkan oleh *Institute of Electrical and Electronics Engineers (IEEE)*, yang disebut *WirelessMANTM*, memberikan perspektif baru dalam mengakses *internet* dengan kecepatan tinggi tanpa tergantung pada jaringan kabel atau *modem*. Tahun 2002 terbentuk forum *Worldwide Interoperability for Microwave Access (WiMAX)* yang mengacu pada standar 802.16 dan bertugas menginterkoneksi berbagai standar teknis yang bersifat global menjadi satu kesatuan. Teknologi *WiMAX* lebih murah dibandingkan dengan teknologi *broadband* lain seperti *digital subscriber line (DSL)* atau kabel *modem*.

Kecepatan koneksi atau kemajuan teknologi yang baru bukan hanya aspek yang penting yang harus dievaluasi, tetapi keduanya merupakan fakta transmisi *wireless* yang tidak aman untuk berkomunikasi. Aspek keamanan merupakan hal yang sangat penting untuk teknologi *broadband* dalam mengakses informasi dari *internet*. Dalam tulisan ini dibahas tentang perkembangan *WiMAX*, perbedaannya dengan *WiFi*, fitur-fitur yang ada serta sistem keamanan yang terdapat pada teknologi *WirelessMANTM* berdasarkan pada spesifikasi standar 802.16.

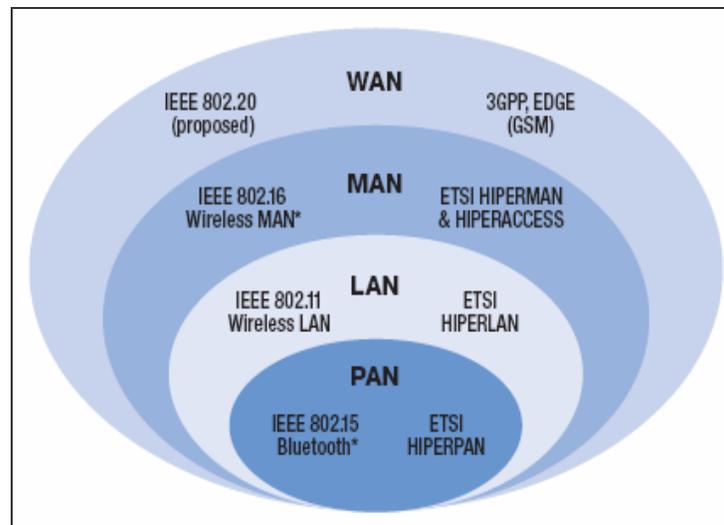
Standar *IEEE* 802.16 memberikan kemudahan dalam akses *internet* untuk *area metropolitan* dengan hanya mendirikan beberapa *base station (BS)* yang dapat meng-coverage jutaan *subscriber (SS)*. Teknologi *WiMAX* merupakan solusi untuk kota atau daerah pedesaan yang belum berkembang dalam penyediaan akses *internet*. Enkripsi data yang digunakan berupa *data encryption standar (DES)* dan *authentication* pada setiap *client/subscriber station (SS)* yang sangat baik dengan sertifikat *X.509* yang unik, handal dan dapat dipercaya ketangguhannya.

Kata Kunci : *IEEE 802.16 / WirelessMANTM / (WiMAX), wireless, security, broadband, subscriber station (SS), base station (BS), DES, MAC dan PHY.*

1. Pendahuluan

1.1 Pengertian *WiMAX*

Worldwide Interoperability for Microwave Access (WiMAX) merupakan standar industri yang bertugas menginterkoneksi berbagai standar teknis yang bersifat global menjadi satu kesatuan. *WiMAX* dan *WiFi* dibedakan berdasarkan standar teknik yang bergabung didalamnya. *WiFi* menggabungkan standar *IEEE 802.11* dengan *ETSI HiperLAN* yang merupakan standar teknis yang cocok untuk keperluan *WLAN*, sedangkan *WiMAX* merupakan penggabungan antara standar *IEEE 802.16* dengan *ETSI HiperMAN*^[4]. Standar keluaran *IEEE* banyak digunakan secara luas di daerah asalnya, yaitu Eropa dan sekitarnya. Untuk dapat membuat teknologi ini digunakan secara global, maka diciptakan *WiMAX*. Standar global yang dipakai di dunia dapat digambarkan sebagai berikut.



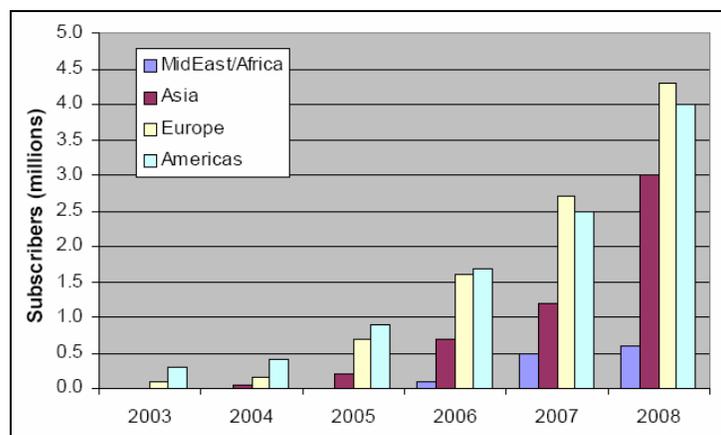
Gambar 1 Standar-standar yang ada dengan spesifikasi yang mendukung komunikasi sampai tingkat *MAN* disatukan dengan standar *WiMAX* ^[1]

Kedua standar yang disatukan ini merupakan standar teknis yang memiliki spesifikasi yang sangat cocok untuk menyediakan koneksi berjenis *broadband* lewat media *wireless* atau *broadband wireless access (BWA)*. Pada masa mendatang, segala sesuatu yang berhubungan dengan teknologi *BWA* kemungkinan akan diberi sertifikasi *WiMAX*. Standar *WiMAX* dibentuk oleh gabungan-gabungan industri perangkat *wireless* dan *chip-chip* komputer diseluruh dunia. Perusahaan besar ini bergabung dalam suatu forum kerja yang merumuskan standar interkoneksi antar teknologi *BWA* yang mereka miliki pada produk-produknya.

1.2 Standar IEEE 802.16 (WiMAX)

Terobosan jaringan *internet wireless* sebentar lagi akan menjadi kenyataan. Dengan *tower* yang dipasang dipusat akses *internet (hot spot)* di tengah kota *metropolitan*, seorang pemakai *laptop*, komputer, *handphone*, hingga *personal digital assistant (PDA)*, dengan *wireless card* bisa koneksi dengan *internet*, bahkan di tengah sawah atau pedesaan yang masih dalam cakupan *area* 50 kilometer. Hal ini dapat terjadi karena teknologi *WiMAX* yang menggunakan standar baru *IEEE 802.16*. Saat ini *WiFi* menggunakan standar komunikasi *IEEE 802.11*. Yang paling banyak dipakai adalah *IEEE 802.11b* dengan kecepatan 11 Mbps, hanya mencapai cakupan *area* tidak lebih dari ratusan meter saja. *WiMAX* merupakan saluran komunikasi radio yang memungkinkan terjadinya jalur *internet* dua arah dari jarak puluhan kilometer. Dengan memanfaatkan gelombang radio, teknologi ini bisa dipakai dengan frekuensi berbeda, sesuai dengan kondisi dan peraturan pemakaian frekuensi di negara *user*^[4].

Pada awalnya *standard IEEE 802.16* beroperasi ada frekuensi 10-66 GHz dan memerlukan *tower line of sight*, tetapi pengembangan *IEEE 802.16a* yang disahkan pada bulan Maret 2004, menggunakan frekuensi yang lebih rendah yaitu sebesar 2-11 GHz, sehingga mudah diatur, dan tidak memerlukan *line-of-sight*. Cakupan *area* yang dapat *discovery* sekitar 50 km dan kecepatan *transfer data* sebesar 70 Mbps. Pengguna tidak akan kesulitan dalam mengulur berbagai macam kabel, apalagi *WiMAX* mampu menangani sampai ribuan pengguna sekaligus. Prediksi perkembangan pemakai yang menggunakan *WiMAX* akan terus berkembang dari tahun ke tahun seperti terlihat pada Gambar 2 berikut ini.



Gambar 2 Grafik prediksi perkembangan penggunaan *WiMAX* di berbagai benua dari tahun ketahun^[3]

Intel akan mulai memasang antena luar ruangan *WiMAX* sebagai tahap pengembangan *WiFi*. Teknologi *WiFi* dan *WiMAX* akan saling melengkapi. *WiFi* untuk jangkauan jarak dekat di seputar kampus atau kantor sedangkan *WiMAX* untuk memfasilitasi sebuah kota dengan akses *wireless internet*. Pada akhirnya, diperkirakan hampir semua *laptop*, *PDA*, dan piranti *information and communication technology (ICT)* lainnya akan *compatible* dengan fitur *WiFi* dan *WiMAX*.

1.3 Keuntungan *WiMAX*

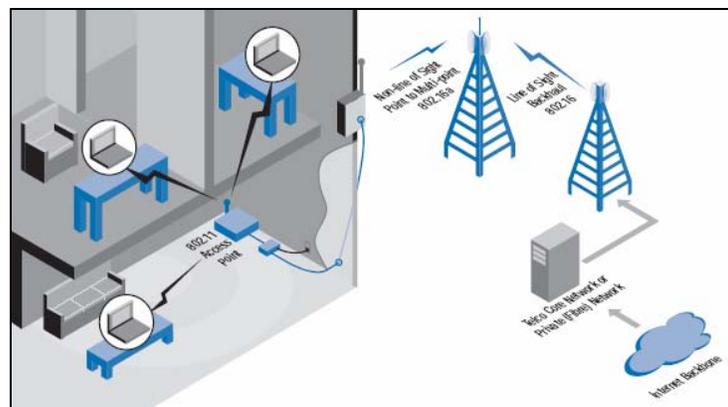
Ada beberapa keuntungan dengan adanya *WiMAX*, jika dibandingkan dengan *WiFi* antara lain sebagai berikut^[4].

1. Para produsen mikroelektronik akan mendapatkan lahan baru untuk dikerjakan, dengan membuat *chip-chip* yang lebih *general* yang dapat dipakai oleh banyak produsen perangkat *wireless* untuk membuat *BWA*-nya. Para produsen perangkat *wireless* tidak perlu mengembangkan solusi *end-to-end* bagi penggunaanya, karena sudah tersedia standar yang jelas.
2. Operator telekomunikasi dapat menghemat investasi perangkat, karena kemampuan *WIMAX* dapat melayani pelanggannya dengan area yang lebih luas dan dengan kompatibilitas yang lebih tinggi.
3. Pengguna akhir akan mendapatkan banyak pilihan dalam berinternet. *WiMAX* merupakan salah satu teknologi yang dapat memudahkan kita untuk koneksi dengan *internet* secara mudah dan berkualitas.
5. Memiliki banyak fitur yang selama ini belum ada pada teknologi *WiFi* dengan standar *IEEE 802.11*. Standar *IEEE 802.16* digabungkan dengan *ETSI HiperMAN*, maka dapat melayani pangsa pasar yang lebih luas.
6. Dari segi *coverage*-nya saja yang mencapai 50 kilometer maksimal, *WiMAX* sudah memberikan kontribusi yang sangat besar bagi keberadaan *wireless MAN*. Kemampuan untuk menghantarkan data dengan *transfer rate* yang tinggi dalam jarak jauh dan akan menutup semua celah *broadband* yang tidak dapat terjangkau oleh teknologi kabel dan *digital subscriber line (DSL)*.
7. Dapat melayani para *subscriber*, baik yang berada pada posisi *line of sight (LOS)* maupun yang memungkinkan untuk tidak *line of sight (NLOS)*.

WiMAX memang dirancang untuk melayani baik para pengguna yang memakai *antenna* tetap (*fixed wireless*) maupun untuk yang sering berpindah-pindah tempat (*nomadic*). *WiMAX* tidak

hanya hanya dapat melayani para pengguna dengan *antenna* tetap saja misalnya pada gedung-gedung diperkantoran, rumah tinggal, toko-toko dan sebagainya. Bagi para pengguna *antenna indoor*, *notebook*, *PDA*, *PC* yang sering berpindah tempat dan banyak lagi perangkat *mobile* lainnya memang telah kompatibel dengan dengan standar-standar yang dimiliki *WiMAX*.

Perangkat *WiMAX* juga mempunyai ukuran kanal yang bersifat fleksibel, sehingga sebuah *BTS* dapat melayani lebih banyak pengguna dengan *range* spektrum frekuensi yang berbeda-beda. Dengan ukuran kanal spektrum yang dapat bervariasi ini, sebuah perangkat *BTS* dapat lebih fleksibel dalam melayani pengguna. *Range* spektrum teknologi *WiMAX* termasuk lebar, dengan didukung dengan pengaturan kanal yang fleksibel, maka para pengguna tetap dapat terkoneksi dengan *BTS* selama mereka berada dalam *range* operasi dari *BTS*. Fasilitas *quality of service (QoS)* juga diberikan oleh teknologi *WiMAX* ini. Sistem kerja *media access control* pada *data link layer* yang *connection oriented* memungkinkan digunakan untuk komunikasi *video* dan suara. Pemilik *internet service provider (ISP)* juga dapat membuat berbagai macam produk yang dapat dijual dengan memanfaatkan fasilitas ini, seperti membedakan kualitas servis antara pengguna rumahan dengan pengguna tingkat perusahaan, membuat *bandwidth* yang bervariasi, fasilitas tambahan dan masih banyak lagi.



Gambar 3 Sebuah *BTS WiMAX* dapat digunakan sebagai *backhaul* untuk titik-titik *hotspot* ^[1]

Standar *IEEE 802.16* merupakan keluaran dari organisasi *IEEE*, sama seperti *IEEE 802.11* adalah standar yang dibuat khusus untuk mengatur komunikasi lewat media *wireless*. Yang membedakannya adalah *WiMAX* mempunyai tingkat kecepatan *transfer* data yang lebih tinggi dengan jarak yang lebih jauh, sehingga kualitas layanan dengan menggunakan komunikasi ini

dapat digolongkan ke dalam kelas *broadband*. Standar ini sering disebut *air interface for fixed broadband wireless access system* atau *interface* udara untuk koneksi *broadband*^[4].

Sebenarnya standarisasi *IEEE 802.16* ini lebih banyak mengembangkan hal-hal yang bersifat teknis dari *layer physical* dan *layer datalink (MAC)* dari sistem komunikasi *BWA*. Versi awal dari standar *802.16* ini dikeluarkan oleh *IEEE* pada tahun 2002. Pada bersi awalnya, perangkat *802.16* beroperasi dalam lebar frekuensi 10-66 GHz dengan jalur komunikasi antar perangkatnya secara *line of sight (LOS)*. *Bandwidth* yang diberikan oleh teknologi ini sebesar 32-134 Mbps dalam *area coverage* maksimal 5 kilometer. Kapasitasnya dirancang mampu menampung ratusan pengguna setiap satu *BTS*. Dengan kemampuan semacam ini teknologi perangkat yang menggunakan standar *802.16* cocok digunakan sebagai penyedia koneksi *broadband* melalui *media wireless*. Perbedaan teknis antara *IEEE 802.11* dengan *IEEE 802.16* dapat dilihat pada Tabel 1 berikut ini.

Tabel 1 Perbedaan teknologi *IEEE 802.11* dengan *IEEE 802.16* ^[4]

	IEEE 802.11	IEEE 802.16	Perbedaan Teknis
Jarak	Dibawah 9 Km	Hingga 50 Km	Teknik 256 FFT sistem <i>signalingnya</i> menciptakan fitur ini.
Coverage	Optimal jika bekerja di dalam ruangan	Dirancang untuk penggunaan diluar ruangan dengan kondisi <i>NLOS</i>	<i>IEEE 802.16</i> memiliki sistem gain yang lebih tinggi, mengakibatkan sinyal lebih kebal terhadap halangan dalam jarak yang lebih jauh.
Skalabilitas	Skala penggunaannya hanya dalam tingkat <i>LAN</i> . Ukuran frekuensi kanalnya dibuat <i>fix</i> (20 MHz)	Dibuat untuk mendukung sampai 100 pengguna. Ukuran frekuensi kanal dapat bervariasi mulai dari 1,5 sam-pai dengan 20 MHz.	Sistim <i>TDMA</i> dan peng-aturan <i>slot</i> komunikasi, sehingga semua frekuensi yang termasuk dalam <i>range IEEE 802.16</i> dapat dipakai serta jumlah pengguna dapat bertambah.
Bit Rate	2,7 bps/Hz hingga 54Mbps dalam kanal 20 MHz	5 bps/Hz hingga 100 Mbps dalam kanal 20 MHz.	Teknik modulasi yang lebih canggih disertai koreksi <i>error</i> yang lebih fleksibel, sehingga penggunaan freku-ensi kanal lebih <i>effisien</i> .
QoS	Tidak mendukung <i>QoS</i>	<i>QoS</i> dibuat dalam <i>layer MAC</i>	Adanya pengaturan secara otomatis terhadap slot-slot <i>TDMA</i> , sehingga dimanfaatkan untuk peng-aturan <i>QoS</i> .

1.4 Varian-Varian *IEEE 802.16*

Varian-varian *WiMAX* dimaksudkan untuk mengembangkan *performance* dan kemampuan dari teknologi yang digunakannya, agar menjadi lebih hebat dan dapat meluas penggunaannya. Untuk

mengembangkan jangkauan dan daya jualnya, maka standar *IEEE* 802.16 direvisi menjadi *IEEE* 802.16a. Standar teknis *IEEE* 802.16a inilah yang banyak digunakan oleh perangkat-perangkat dengan sertifikasi *WiMAX*.

Selain *IEEE* 802.16a, varian lainnya adalah *IEEE* 802.16b yang banyak menekankan segala keperluan dan permasalahan dengan *quality of service (QoS)*, *IEEE* 802.16c banyak menekankan pada *interoperability* dengan protokol-protokol lain, *IEEE* 802.16d merupakan revisi dari *IEEE* 802.16c ditambah dengan kemampuan untuk *access point*, serta *IEEE* 802.16d menekankan pada masalah mobilitas. Varian-varian standar *IEEE* 802.16 dapat dilihat pada Tabel 2 berikut ini.

Tabel 2 Varian-varian standar *IEEE* 802.16 ^[4]

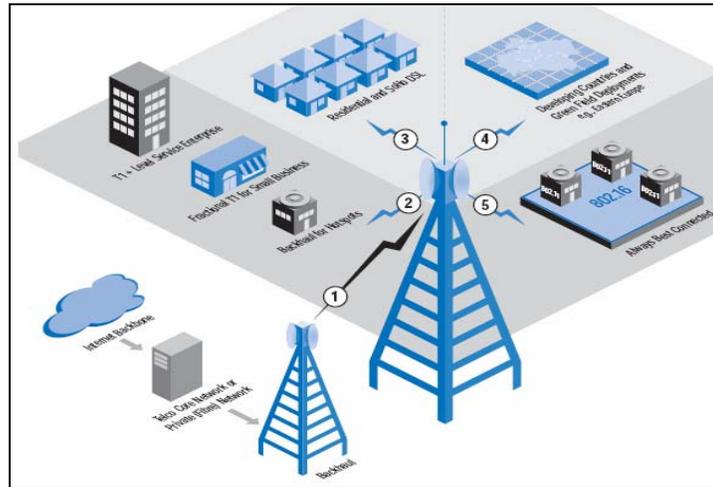
	IEEE 802.16	IEEE 802.16a	IEEE 802.16e
Terstandarisasi	Januari 2002	Januari 2003 (<i>IEEE</i> 802.16a)	Estimasi pertengahan 2004
Spektrum	10 – 66 GHz	2 – 11 GHz	< 6 GHz
Kondisi Kanal	<i>Line Of Sight</i>	<i>Non Line Of Sight</i>	<i>Non Line Of Sight</i>
Bit Rate	32 sampai 134 Mbps menggunakan frekuensi kanal 28 MHz	Hingga 70 Mbps menggunakan frekuensi kanal 20 Mhz	Hingga 15 Mbps menggunakan frekuensi kanal 5 MHz
Modulasi	<i>QPSK</i> , 16 QAM dan 64 QAM	<i>OFDM</i> 256 sub-carrier, <i>QPSK</i> , 16 QAM, 64 QAM	<i>OFDM</i> 256 sub-carrier, <i>QPSK</i> , 16 QAM, 64 QAM
Mobilitas	Perangkat <i>wireless</i> tetap	Perangkat <i>wireless</i> tetap dan portabel	<i>Nomadic Mobility</i>
Frekuensi Per Kanal	20, 25 dan 28 MHz	Mulai dari 1,5 hingga 20 MHz	Mulai dari 1,5 hingga 20 MHz
Radius Per Cell	2 sampai 5 Km	7 – 10 Km dengan kemampuan maksimal hingga 50 Km	2 – 5 Km

Perubahan yang cukup signifikan pada standar *IEEE* 802.16 untuk membentuk varian *IEEE* 802.16a, adalah lebar frekuensi operasinya. Perbedaan ini dimaksudkan untuk mendukung komunikasi dalam kondisi *line of sight (LOS)*, dan *non line of sight (NLOS)*. Dengan adanya sistem *NLOS*, keterbatasan yang ada pada *WiFi* dapat dikurangi.

Perubahan yang sangat signifikan pada standar 802.16 untuk membentuk varian terletak pada lebar frekuensi operasinya. Standar 802.16 beroperasi pada *range* 10-66 GHz, sedangkan 802.16a menggunakan frekuensi yang lebih rendah, yaitu 2–11 GHz, sehingga memungkinkan komunikasi

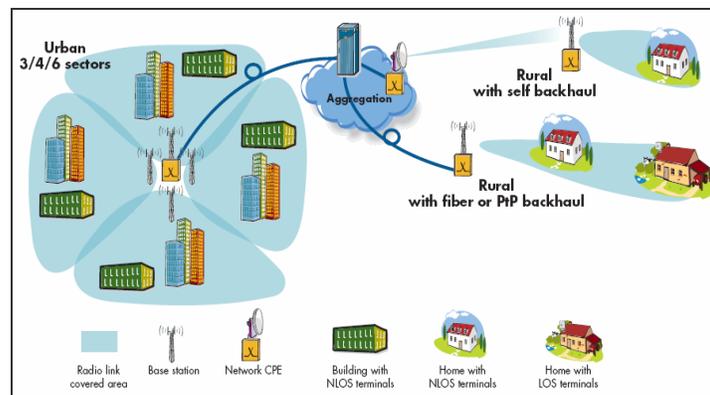
non line of sight (NLOS). Kelemahan dari komunikasi dengan frekuensi rendah ini adalah semakin kecil kapasitas *bandwidth* dari koneksi yang dilakukannya. Ukuran kanal-kanal frekuensi yang fleksibel dengan *range* yang lebar, merupakan keunggulan dari 802.16a.

Aplikasi standar *WiMAX* untuk berbagai keperluan ditunjukkan pada Gambar 4 dibawah ini.



Gambar 4 Teknologi *WiMAX* memungkinkan aplikasinya yang luas untuk berbagai keperluan [1]

Beberapa topologi dan pilihan *backhauling* telah didukung oleh teknologi *WiMAX*, antara lain saluran kabel *backhauling* (*typically over Ethernet*), dan koneksi *point to point*. Pada Gambar 5 di bawah ini terlihat empat buah *base station (BS)* meng-coverage 4 sektor/kawasan, sebuah *repeater* sebagai pengumpulan (*aggregation*) sinyal yang akan dikirimkan ke wilayah pedesaan (*rural area*). Komunikasi antar *base station (BS)* dapat menggunakan *wireless* maupun *optical fiber*.



Gambar 5 Topologi *WiMAX* dalam *area* perkotaan dan pedesaan [6]

Selain perubahan frekuensi operasi, pada *layer physical* dari standar *IEEE 802.16a* ditambahkan tiga spesifikasi baru untuk mendukung fitur *NLOS*-nya ini, yaitu *single carrier PHY*, *256 FFT OFDM PHY* dan *2048 FFT OFDM PHY*. Format sinyaling *OFDM* dipilih dalam standar ini dimaksudkan agar teknologi ini dapat bersaing dengan *competitor* utamanya yaitu teknologi *CDMA*, yang juga bekerja dalam sistem *NLOS*. Fitur-fitur lain yang ada pada standar *IEEE 802.16a* adalah sebagai berikut^[6].

1. Untuk menghantarkan jaringan komunikasi yang berkualitas dengan jangkauan yang luas adalah lebar kanal frekuensi yang fleksibel.
2. *Burst profile* yang dapat beradaptasi (fasilitas *burst* adalah cirri khas dari teknologi *broadband*).
3. *Forwarding error correction (FEC)* untuk mengoreksi jika terjadi kesalahan.
4. *Advanced antenna system* untuk meningkatkan wilayah jangkauan.
5. Kapasitas dan kekebalan terhadap interferensi dari sinyal lain.
6. *Dynamic frequency selection (DFS)*, pemilihan frekuensi kanal secara dinamis dan juga berfungsi untuk mengurangi interferensi.
7. *Space time coding (STC)* yang akan meningkatkan *performance* dalam *area* batas pinggir dari sinyal yang dipancarkan oleh sebuah *base station (BS)*.

Selain *layer physical (PHY)*, standar ini juga menentukan seperangkat aturan yang berada pada *layer data link (MAC)*. Standar ini digunakan untuk melayani pengguna dalam sistem *point to multi point*. Standar *IEEE 802.16a* menggunakan sistem *slot* koneksi yang ada dalam protokol *time division multiple access (TDMA)*. Pengaturan *slot* koneksi ini diatur oleh *BTS* untuk melayani para pengguna yang ingin terkoneksi dengannya. Fitur-fitur *physical layer (PHY)* ditunjukkan pada Tabel 3.

Tabel 3 Fitur-fitur *physical layer* teknologi *IEEE 802.16 WiMAX* ^[4]

No	Fitur	Keuntungan
1	Menggunakan sistem sinyaling 256 <i>point FFT OFDM</i> .	Mendukung sistem <i>multipath</i> untuk memungkinkan diaplikasikan pada area terbuka (<i>outdoor</i>) dengan kondisi LOS dan NLOS.
2	Ukuran kanal frekuensi yang fleksibel (misalnya 3,5 MHz, 5 MHz, 19 MHz)	Menyediakan fleksibilitas yang memungkinkan komunikasi beroperasi menggunakan kanal-kanal frekuensi yang bervariasi sesuai dengan kebutuhan.
3	Didesain untuk dapat mendukung sistem <i>smart antenna</i>	Dengan menggunakan <i>smart antenna</i> yang lebih nyaman digunakan sehari-hari, interferensi dapat ditekan dan <i>gain</i> dapat ditingkatkan.
4	Mendukung <i>TDD</i> dan <i>FDD Duplexing</i>	Menangani masalah bervariasinya regulasi-regulasi diseluruh dunia.

5	Sistem modulasi yang fleksibel dengan sistem <i>error correction</i> yang bervariasi setiap <i>RF burst</i>	Memungkinkan terjalannya koneksi yang <i>reliable</i> , memberikan <i>transfer rate</i> yang maksimal kepada setiap <i>subscriber</i> yang terkoneksi dengannya.
---	---	--

Layer media access control (MAC) dari standar *IEEE 802.16* ini didesain untuk dapat membawa dan mengakomodasi segala macam protokol di atasnya, seperti *ATM*, *Ethernet* atau *internet protokol (IP)*. Fitur-fitur *media access control layer* ditunjukkan pada Tabel 4 berikut ini.

Tabel 4 Fitur-fitur *MAC layer* teknologi *IEEE 802.16 WiMAX* ^[4]

No	Fitur	Keuntungan
1	<i>Connection oriented</i>	Proses <i>routing</i> dan paket <i>forwarding</i> yang lebih <i>reliable</i> .
2	<i>Automatic retransmisi request (ARQ)</i>	Meningkatkan <i>performance end to end</i> dengan menyembunyikan <i>error</i> pada <i>layer RF</i> yang dibawa dari <i>layer</i> di atasnya.
3	<i>Automatic power control</i>	Memungkinkan pembuatan topologi <i>celluler</i> dengan <i>power</i> yang dapat terkontrol secara otomatis.
4	<i>Security dan encryption</i>	Melindungi privasi dari para <i>subscriber</i>
5	Mendukung sistem modulasi <i>adaptive</i>	Memungkinkan <i>data rate</i> yang lebih tinggi
6	<i>Scalability</i> yang tinggi hingga mendukung 100 <i>subscriber</i>	Biaya penggunaan yang sangat efektif, karena mampu menampung pengguna dalam jumlah yang besar.
7	Mendukung sistem <i>quality of service (QoS)</i>	Dapat memberikan <i>latency</i> rendah pada aplikasi-aplikasi <i>delay sensitive</i> , seperti <i>VoIP</i> dan <i>streaming video</i> .

2. Implikasi Keamanan Pada Teknologi *Wirelessmantm* (Standar Ieee 802.16)

2.1 Prinsip Kerja Teknologi *WirelessMANTM*

Teknologi *WirelessMANTM / IEEE 802.16 / WiMAX* dapat meng-cover area sekitar 50 kilometer, dimana ratusan pelanggan akan di-share sinyal dan kanal untuk mentransmisikan data dengan kecepatan sampai 155 Mbps. Aspek keamanan merupakan aspek yang sangat penting dan akan dievaluasi oleh para pengguna *internet* dengan menggunakan fasilitas *ADSL* atau teknologi kabel *modem* maupun yang berlangganan dengan teknologi *WiMAX*.

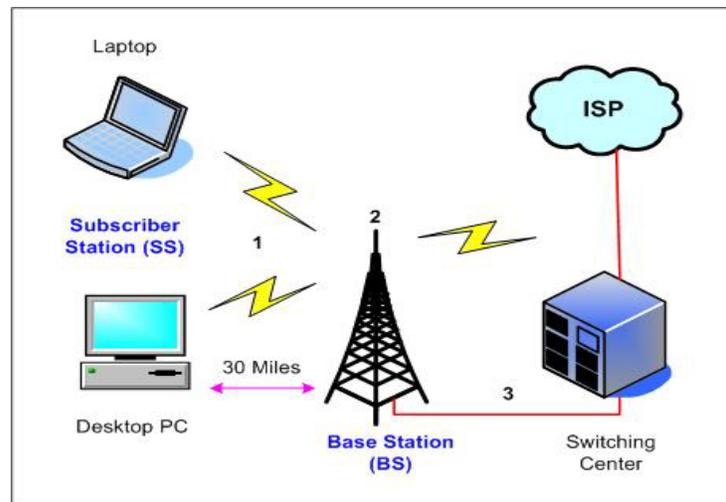
Sistem pengamanan data dilakukan pada *layer physical (PHY)* dan *data link layer (MAC)* pada suatu arsitektur jaringan, tepatnya pada *base station (BS)* untuk didistribusikan ke wilayah

sekelilingnya dan *subscriber station (SS)* untuk komunikasi *point to multipoint*. *Base station (BS)* dihubungkan secara langsung dengan jaringan umum (*public network*).

Secara umum *WirelessMANTM traffic* dibedakan menjadi tiga bagian, seperti berikut ini ^[4].

1. Pelanggan mengirimkan data dengan kecepatan 2 – 155 Mbps dari *subscriber station (SS)* ke *base station (BS)*.
2. *Base station* akan menerima sinyal dari berbagai pelanggan dan mengirimkan pesan melalui *wireless* atau kabel ke *switching center* melalui protokol IEEE 802.16.
3. *Switching center* akan mengirimkan pesan ke *internet service provider (ISP)* atau *public switched telephone network (PSTN)*.

Ketiga bagian tersebut di atas secara blok dapat dilihat pada Gambar 6 dibawah ini.



Gambar 6 *Traffic* yang terjadi pada *WiMAX* ^[5]

Pada Gambar 6 di atas *laptop* dan *desktop personal computer (PC)* berfungsi sebagai *subscriber station (SS)*, *tower antenna* beserta perangkatnya sebagai *base station (BS)* dan *switching center* sebagai pengatur pilihan koneksi ke *internet service provider (ISP)*.

2.2 Ancaman Umum

Dalam teknologi *WiMAX / WirelessMANTM*, sebuah *base station (BS)* akan meng-coverage seluruh wilayah kota yang terdiri atas ratusan / jutaan pelanggan (*subscriber*). Semua pelanggan akan menggunakan media yang sama (*sharing*) berupa udara untuk mentransfer data.

Teknologi yang digunakan untuk komunikasi antara *subscriber station (SS)* dan *base station (BS)* menggunakan teknologi *time division multiple access (TDMA)*. Untuk menjamin *confidentiality* data pada pelanggan maka pengiriman / penerimaan data dari *subscriber station (SS)* dan *base station (BS)* dienkripsi menggunakan *X.509* yang disertifikasi oleh *RSA*. Ancaman yang umum pada pelanggan berdasarkan teknologi *WirelessMANTM* adalah sebagai berikut ^[4].

1. Pencurian sinyal atau layanan.
2. Pencurian data *user*.
3. *Cloning*.

Dalam standar *IEEE 802.16* digunakan metode untuk meningkatkan keamanan yang berupa *authentication*, *authorization* dan *encryption*. *Authentication* yang digunakan pada *subscriber station (SS)* adalah *X.509* dengan *RSA public key cryptography standard (PKCS)*.

Authentication dan *authorization* pada *subscriber station* digunakan *X.509* dengan kunci publik untuk mengidentifikasi informasi, misalnya *UserID*, *SS's name* dan lain sebagainya. Informasi ini akan terus teridentifikasi selama komunikasi antara *subscriber station (SS)* dan *base station (BS)* masih berlangsung. *Encryption* yang digunakan dalam standar *IEEE 802.16* adalah *56-bit DES* pada mode *cyclic block chaining (CBC)*. Kesalahan yang terjadi pada *ciphertext* tidak dipropagasikan ke dalam *plaintext* dengan menerapkan algoritma *multiple encryption*.

2.3 Subscriber Station (SS) Authentication dan Registrasi

Setiap *subscriber station (SS)* terdiri dari dua buah sertifikasi yaitu *X.509* dan sertifikasi dari perusahaan. Sertifikasi yang menghubungkan antara *48-bit MAC SS* dan kunci *RSA* dikirimkan dari *base station* ke *subscriber station(SS)* dalam bentuk *authorization request(AR)* dan *authentication information (AI)*. Setelah berhasil melakukan proses *authentication* dan *authorization* maka *subscriber station (SS)* akan tercatat dalam jaringan dan *subscriber* akan menerima sebuah *IP address* dari *server DHCP* dan dapat mengakses *WirelessMANTM*.

2.4 Struktur Layer

Layer pertama adalah *physical layer (PHY)*, jalur frekuensi, modulasi, teknik pengkoreksi kesalahan, sinkronisasi antara pemancar dan penerima dan struktur *time division multiplexing (TDM)*. *Layer* di atasnya berfungsi untuk menyediakan pelayanan kepada *subscriber*, misalnya transmisi data dalam *frame*, pengontrolan media akses, pengelompokan kedalam *media access control (MAC)*. *MAC* bertanggung jawab tentang bagaimana dan kapan *base station (BS)* atau *subscriber station (SS)* mentransmisikan sinyal melalui kanal.

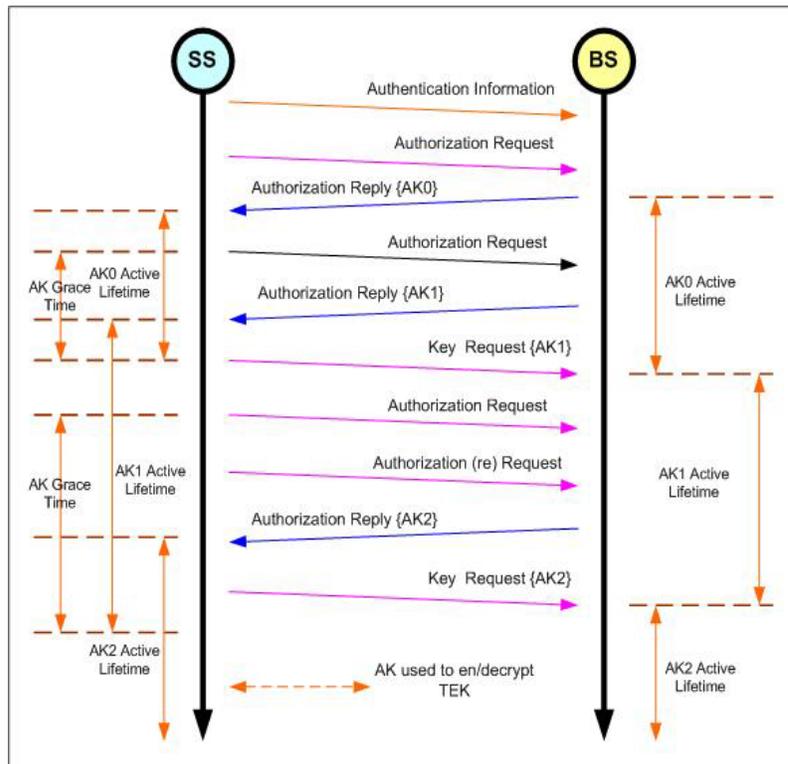
2.5 Privasi Sublayer

Privasi *sublayer* menyediakan sistem pengamanan data dengan enkripsi diantara *base station (BS)* dan *subscriber station (SS)*. *Base station (BS)* memproteksi pengaksesan data dengan cara enkripsi pada seluruh jaringan. Dalam privasi *sublayer* dibedakan menjadi dua protokol sebagai berikut ^[5].

1. Enkapsulasi protokol yang akan bertanggung jawab terhadap data yang melewati jaringan *broadband wireless access (BWA)*.
2. Protokol *key management (privacy key management or PKM)* yang menyediakan keamanan distribusi antara *base station (BS)* dan *subscriber station (SS)*.

2.6 Protokol Privacy Key Management (PKM)

Protokol *privacy key management (PKM)* digunakan untuk mengamankan data antara *subscriber station* dan *base station*. Pada saat *subscriber station (SS)* menginginkan *login* ke *base station (BS)*, maka akan mengirimkan pesan *authentication information (AI)* ke *base station (BS)*, seperti terlihat pada gambar dibawah ini.



Gambar 7 Proses *authentication* [5]

Pesan ini terdiri dari kode SS's yang unik berupa sertifikat X.509 yang dikeluarkan oleh perusahaan SS's. Setelah *subscriber station (SS)* memberikan identifikasi ke *base station (BS)*, maka akan mengirimkan pesan *authorization request (AR)*. Pesan *request* dari *base station (BS)* digunakan untuk menjamin akses data jaringan dan keamanan informasi yang didukung dengan adanya enkripsi data dari *subscriber station (SS)*. Pada saat *base station (BS)* menerima pesan *authentication information (AI)* dan *authorization request (AR)*, maka akan segera melakukan validasi identitas SS's dan mengecek permintaan. Apabila permintaan diperbolehkan, maka *base station (BS)* akan mengeluarkan sebuah *security association identity (SAID)* dengan *requesting SS* dan sebuah *authorization key (AK)* yang telah dienkripsi dengan *SS's public key*

Pesan *request* dari *base station (BS)* digunakan untuk menjamin akses data jaringan dan keamanan informasi yang didukung dengan adanya enkripsi data dari *subscriber station (SS)*. Pada saat *base station (BS)* menerima pesan *authentication information (AI)* dan *authorization request (AR)*, maka akan segera melakukan validasi identitas SS's dan mengecek permintaan. Apabila permintaan diperbolehkan, maka *base station (BS)* akan mengeluarkan sebuah *security association identity (SAID)* dengan *requesting SS* dan sebuah *authorization key (AK)* yang telah dienkripsi dengan *SS's public key*.

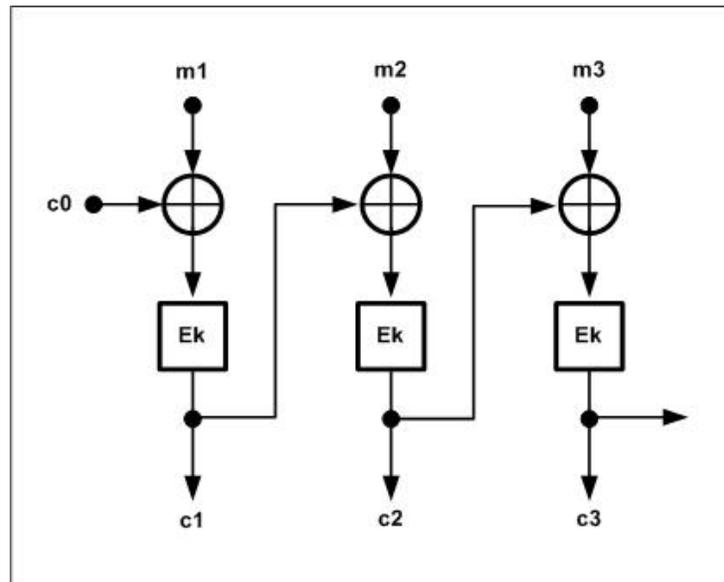
Sebelum *current key* habis masa berlakunya, maka *subscriber station (SS)* meminta lagi *authorization* yang baru dari *base station (BS)* untuk menghindari gangguan yang mungkin terjadi. Protokol *PKM* menyerupai model *client server*, dimana *subscriber station (SS)* adalah *PKM client* dan *base station (BS)* merupakan *PKM server*. Protokol *PKM* menggunakan kunci publik *cryptography* untuk membuat *authorization* antara *subscriber station (SS)* dan *base station (BS)*.

2.7 Security Association (SA)

Protokol *PKM* berdasarkan konsep *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 lain sebagainya.

Setiap pelayanan memerlukan asosiasi keamanan. Untuk *subscriber station (SS)* menggunakan *traffic encryption (TEK) state machine* untuk setiap asosiasi keamanan. *TEK* akan bertanggung jawab untuk manajemen 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)*, seperti ditunjukkan pada Gambar 8. 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 eksklusif, 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)*.



Gambar 8 Proses enkripsi data [8]

Pada Gambar di atas, *plaintext* di-*XOR*-kan dengan blok *chipertext* kemudian di enkripsi, agar informasinya *secure* sehingga tidak mudah diketahui oleh orang lain yang tidak berhak.

2.8 Kunci Pemeliharaan *Base Station (BS)* dan *Subscriber Station (SS)*

Base station (BS) bertanggung jawab dalam pemeliharaan informasi untuk semua *security association (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)*. *Authorization key (AK)* akan aktif sampai waktu yang ditentukan berakhir sesuai dengan batas waktu *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*.

2.9 Metode *Cryptography*

Pertama kali didesain, protokol *privacy key management (PKM)* telah dirancang menggunakan X.509 sertifikasi *digital* dengan kunci publik *RSA* untuk enkripsi, *subscriber station (SS)* *authentication* dan pengubahan kunci otorisasi. Untuk enkripsi data digunakan *data encryption standar (DES)* dengan *chiper block chaining (CBC) 56-bit* untuk standar IEEE 802.16. Inisialisasi vektor *chiper block chaining (CBC)* tergantung dari jumlah *frame* dan perbedaan antar *frame*. Untuk mereduksi jumlah perhitungan intensif pemrosesan kunci publik selama operasi normal, maka pada proses enkripsi digunakan *3DES*.

Protokol *privacy key management (PKM)* untuk otorisasinya menggunakan *hashed message authentication code (HMAC)*. Kelebihan dari enkripsi menggunakan protokol *privacy key management (PKM)* adalah keduanya kokoh (*robust*) dan dibuat dalam bentuk yang standar serta dapat digunakan dalam *platform* yang berbeda (*modular*).

2.10 Implementasi

Sistem komunikasi perangkat *IEEE 802.16 (WiMAX)* agar aman, maka diperlukan tiga hal sebagai berikut ^[7].

1. *Device authentication*

Authentication berkaitan dengan metoda untuk menyatakan bahwa informasinya betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud ^[7]. *Authentication* yang digunakan adalah X.509. *Digital passports* dapat menjamin identifikasi perangkat *IEEE 802.16* seperti *wireless* yang digunakan dalam *access point*.

2. *Data confidentiality (privacy)*

Confidentiality atau *privacy* merupakan hal yang sangat penting untuk jaringan termasuk komunikasi *wireless*. Inti utama aspek *confidentiality* atau *privacy* adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Confidentially* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu, sedangkan *privacy* lebih ke arah data-data yang bersifat privat ^[7].

3. *Data integrity*

Keutuhan data mutlak diperlukan dalam suatu komunikasi *wireless*. Jaminan terhadap keutuhan data dapat dilakukan dengan *digital signature* atau fungsi *hash*.

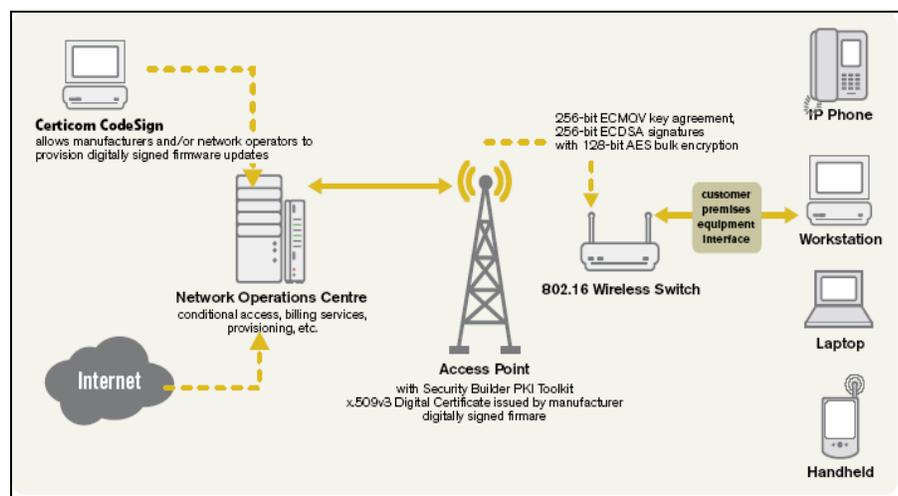
Untuk menambahkan X.509 sertifikasi *digital* untuk *authentication*, *security builder PKI toolkit* dapat digunakan seperti berikut ini [2].

1. *Generate RSA, ECC dan Diffie-Hellman (DH) private/public keys.*
2. *Generate certificate request (PKCS #10).*
3. Sertifikasi *parsing* dan ekstraksi kunci publik.
4. *Generate shared secret keys (AES, 3DES, RC2, RC4).*
5. *Securely transport shared secrets* menggunakan *RSA, Diffie-Hellman (DH), Elliptic-Curve Menezes Qu Vanstone (ECMQV)* atau *Elliptic-Curve Diffie-Hellman (ECDH)*,
6. *Securely store privacy keys, local identity certificates, and trusted root certificates.*
7. *Verify code signature for firmware update (PKCS #7).*

Untuk mencapai tingkat keamanan dan efisiensi yang tinggi, maka untuk teknologi *WiMAX* sebaiknya menggunakan seperti berikut ini [2].

1. *128 bit advanced encryption standard (AES)* untuk kecepatan dan enkripsi simetrik untuk menjaga *confidentiality*,
2. *HMAC-SHA-1* algoritma *hash* untuk kecepatan dan keutuhan data.
3. *256-bit ECMQV* untuk kecepatan dan keamanan data, *authentication* dan *transport* menggunakan *128-bit AES*.

Untuk pengamanan data teknologi *WiMAX* menurut *Certicom* [2], dapat digambarkan seperti Gambar 9. Pengamanan komunikasi *wireless* jalur lebar (*broadband*) dilakukan dari jaringan *internal* sampai dengan terkoneksi ke jaringan *internet*.



Gambar 9 Implementansi sistem keamanan pada *WiMAX* standar [2]

3. Penutup

3.1 Kesimpulan

Dari pembahasan di atas dapat diambil beberapa kesimpulan sebagai berikut.

1. Akhir-akhir ini teknologi *wireless* telah berkembang sangat pesat yang menyediakan hubungan telekomunikasi tanpa tergantung dari jaringan kabel menggunakan telepon atau TV kabel. Dengan adanya teknologi *WirelessMANTM* maka akan memberikan kemurahan dan kecepatan *transfer* data dengan akses *internet* jalur lebar (*broadband*).
2. Standar *IEEE 802.16* memberikan kemudahan dalam akses *internet* untuk *area metropolitan* dengan menerapkan beberapa *base station (BS)* yang dapat meng-coverage jutaan *subscriber station (SS)*.
3. Teknologi *WiMAX* merupakan salah satu solusi untuk dapat mengembangkan teknologi informasi dalam suatu kota atau pedesaan karena jangkauannya sampai jarak 50 km, sehingga memungkinkan untuk meng-coverage seluruhnya.
4. Meskipun tidak didesain untuk menggeser jaringan lokal (*LAN*), standar *IEEE 802.16* menyediakan fitur untuk pengembangan 802.11, sehingga saling melengkapi.
5. Standar *IEEE 802.16* menggunakan *authentication subscriber station (SS)* yang handal. Setiap *subscriber station (SS)* mempunyai sertifikat *X.509* yang unik, handal dan dapat dipercaya ketangguhannya, karena layanan mempunyai kunci yang berbeda.

3.2 Saran

Beberapa hal yang disarankan dalam penulisan makalah tentang sistem keamanan teknologi *WiMAX* ini, adalah sebagai berikut.

1. Mudah-mudahan teknologinya dapat segera terealisasi untuk dipasarkan, mengingat akan kebutuhan masyarakat tentang pentingnya informasi.
2. Diharapkan dapat memanfaatkan sebagian infrastruktur yang sudah ada pada standar *IEEE 802.11* yang sekarang sudah berjalan.

4. Daftar Pustaka

- [1] _____, *IEEE 802.16* and WiMAX, Broadband Wireless Access for Everyone*, http://www.intel.com/ebusiness/pdf/intel/80216_wimax.pdf, Download Tanggal 13 Desember 2004, Jam 06:00 WIB.

- [2] _____, *Certicom Security for 802.16 / WiMAX Integrating Security for Ultra Wideband Equipment*, http://www.certicom.com/download/aid-285/certicom_WiMAXappnote.pdf, Download Tanggal 14 Desember 2004, Jam 23:00 WIB.
- [3] _____, *WiMAX The Critical Wireless Standard*, http://www.eyeforwireless.com/wimax_report.pdf, Download Tanggal 18 Desember 2004, Jam 22:00 WIB.
- [4] Hayri, *WiMAX : Koneksi Broadband Lewat Wireless*, Majalah PC Media Edisi Juli 2004.
- [5] Paranhos. B, *Security Implications in WirelessMANTM Technology (IEEE 802.16 Standard)*, http://www.giac.org/practical/GSEC/Bruno_Paranhos_GSEC.pdf, Download Tanggal 17 Desember 2004, Jam 06:30 WIB.
- [6] Philipe. L, Dietrich. B, Christophe. B, Laurence. F, *WiMAX, Making Ubiquitous High Speed Data Services a Reality*, http://www.alcatel.com/wimax_report.pdf, Download Tanggal 20 Desember 2004, Jam 07:30 WIB.
- [7] Rahardjo. B, *Keamanan Sistem Informasi Berbasis Internet*, PT Insan Komunikasi Indonesia, Bandung, 2001.
- [8] Stalling. W, *Network and Internet Security*, Prentice Hall, Englewood Cliffs, New Jersey, New York, 1995.

Daftar Singkatan

<i>AES</i>	<i>Advanced Encryption Standard</i>
<i>AK</i>	<i>Authorization Key</i>
<i>AR</i>	<i>Authorization Request</i>
<i>BS</i>	<i>Base Station</i>
<i>BWA</i>	<i>Broadband Wireless Access</i>
<i>CBC</i>	<i>Cyclic Block Chaining</i>
<i>CDMA</i>	<i>Code Division Multiple Access</i>
<i>CPE</i>	<i>Customer Premise Equipment</i>
<i>DES</i>	<i>Digital Encryption Standard</i>
<i>DFS</i>	<i>Dynamic Frequency Selection</i>
<i>DSL</i>	<i>Digital Subscriber Line</i>
<i>ETSI</i>	<i>European Telecommunications Standards Institute</i>
<i>FDD</i>	<i>Frequency Division Duplex</i>
<i>FDX</i>	<i>Full Duplex</i>
<i>FEC</i>	<i>Forwarding Error Correction</i>
<i>Hz</i>	<i>Hertz</i>
<i>IEEE</i>	<i>Institute of Electrical and Electronic Engineers</i>
<i>LAN</i>	<i>Local Area Network</i>
<i>LOS</i>	<i>Line Of Sight</i>
<i>MAC</i>	<i>Media Access Control</i>
<i>MAN</i>	<i>Metropolitan Area Network</i>

<i>NLOS</i>	<i>Non Line Of Sight</i>
<i>OFDM</i>	<i>Orthogonal Frequency Division Multiplexing</i>
<i>PHY</i>	<i>Physical Layer</i>
<i>PKCS</i>	<i>Public Key Cryptography Standar</i>
<i>PKM</i>	<i>Privacy Key Managment</i>
<i>QoS</i>	<i>Quality Of Service</i>
<i>SoHo</i>	<i>Small Office Home Office</i>
<i>SAID</i>	<i>Security Association Identity</i>
<i>STC</i>	<i>Space Time Coding</i>
<i>SS</i>	<i>Subscriber Station</i>
<i>TDD</i>	<i>Time Division Duplex</i>
<i>TDM</i>	<i>Time Division Multiplexing</i>
<i>TDMA</i>	<i>Time Division Multiple Access</i>
<i>TEK</i>	<i>Traffic Encryption</i>
<i>VoIP</i>	<i>Voice Over IP</i>
<i>WiFi</i>	<i>Wireless Fidelity</i>
<i>WiMAX</i>	<i>Worldwide Interoperability for Microwave Access</i>

12. Biografi dan Profil Penulis



Siyamta, adalah salah satu *Staff* Pengajar di Departemen Teknologi Informasi, PPPGT/VEDC Malang, Jawa Timur.

Informasi lebih lanjut dapat dihubungi melalui :

Email : must_yamta@yahoo.com

Tulisan di IlmuKomputer.Com

- Sistem Keamanan Pada *Worldwide Interoperability for Microwave Access (WiMAX)*.
- BerEmail Menggunakan Yahoo! Mail.