Sistem Keamanan pada Teknologi WiMAX

Suharlin

Jurusan Teknik Elektro
Fakultas Teknik - Universitas Jenderal Achmad Yani
e-mail : suharlin_sudarmadji@yahoo.com

ABSTRAK. Worldwide Interoperability for Microwave Access (WiMAX / IEEE 802.16) adalah teknologi wireless, yang merupakan perkembangan dari teknologi *Wireless Fidelity* (WiFi) yang saat ini telah banyak digunakan masyarakat. *Wireless fidelity* (WiFi) menggunakan sistem keamanan sebesar 64 bit dan maksimum 128 bit. Sedangkan sistem keamanan yang dipakai pada WiMAX adalah *Advanced Encryption Standard* (AES) yang dapat mengenkripsi data mulai 128 bit, 192 bit dan 256 bit.

Sistem keamanan yang digunakan dalam WiMAX (IEEE 802.16) berupa *authentication*, *authorization* dan *encryption*. Tingkat keamanan yang dihasilkan mencapai dua kali lipat dibandingkan dengan sistem keamanan yang dihasilkan dalam *Wireless Fidelity* (WiFi). Dengan demikian sistem keamanan pada WiMAX dapat diandalkan oleh para pengguna yang memerlukan tingkat keamanan tinggi dan handal dalam penggunaan internet.

Kata kunci: *IEEE 802.16, AES*

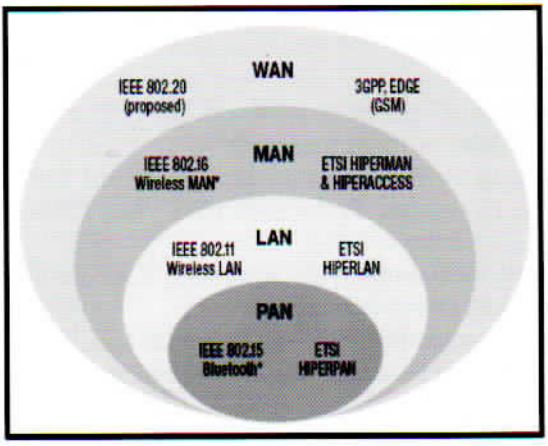
1 Pendahuluan

Worldwide Interoperability for Microwave Access (WiMAX) merupakan standard industri yang bertugas menginterkoneksikan berbagai standard teknis yang bersifat global menjadi satu kesatuan. Standard global yang dipakai merupakan standar teknis yang memiliki spesifikasi teknis yang sangat cocok untuk menyediakan koneksi berjenis broadband lewat media wireless atau *Broadband Wireless Access* (BWA). Teknologi WiMAX yang menggunakan standar baru IEEE 802.16 memungkinkan seorang pemakai laptop, komputer, handphone maupun *Personal Digital Assistant* (PDA), dengan *wireless card* bisa koneksi internet dengan tower yang dipasang di pusat akses internet (*hot spot*) di tengah kota metropolitan , dengan syarat masih dalam cakupan area 50 kilometer dan kecepatan transfer data sebesar 70 Mbps

Tidak seperti jaringan kabel koaxial, WLAN mengirimkan data lewat udara bebas, sehingga sangat memungkinkan diakses di luar batas fisik sebuah kelompok jaringan yang mempunyai hak. Banyak pengembang jaringan wireless yang menyatakan bahwa WLAN mempunyai resiko keamanan yang tinggi. Dan tidak ada jaminan keamanan yang diberikan, kecuali melakukan mitigasi resiko keamanan WLAN yang mungkin dapat dilakukan. Secara garis besar terdapat beberapa isu keamanan jaringan wireless serta resiko pengembangannya yang telah dipublikasikan antara lain serangan terhadap kerahasiaan, integritas data serta ketersediaan jaringan. Untuk menjaga keamanan data yang dikirimkan dengan jaringan wireless, maka WiMAX memakai system keamanan *Advanced Encryption Standard (AES)* yang dapat mengenkripsi data mulai dari 128 bit, 192 bit dan 256 bit.

2 Teknologi WiMAX

WiMAX dan WiFi dibedakan berdasarkan standard teknik yang bergabung didalamnya. WiFi menggabaungkan standar IEEE 802.11 dengan ETSI HiperLAN yang merupakan standar teknis yang cocok untuk keperluan WLAN, sedangkan WiMAX merupakan penggabungan antara standar IEEE 802.11 dengan ETSI HiperMAN. Gambar 1 berikut ini menggambarkan standar-standar yang ada dengan spesifikasi yang mendukung komunikasi sampai tingkat Metropolitan Area Network (MAN) disatukan dengan standar WiMAX.



Gambar 1 Standard-standard MAN dan WiMAX

Standar-standar yang disatukan tersebut merupakan standar teknis yang memiliki spesifikasi yang cocok untuk menyediakan koneksi berjenis broadband lewat media wireless atau Broadband Wireless Access (BWA).

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 dikaver sekitar 50 km dan kecepatan transfer data sebesar 70 Mbps. Pengguna tidak akan kesulitan dalam menggelar berbagai macam kabel, apalagi WiMAX mampu menangani sampai ribuan pengguna sekaligus. Untuk mengembangkan jangkauan dan daya jualnya , maka standar IEEE 802.16 direvisi menjadi IEEE 802.16a. 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.

2.1 Keamanan pada Jaringan Wireless

Keamanan jaringan diperlukan untuk proteksi data selama data tersebut ditransmisikan dan menjamin data tersebut tetap otentik.

Ada 4 syarat yang dibutuhkan komputer dan keamanan jaringan

- Kerahasiaan, data hanya dapat diakses oleh yang berhak
- Ketangguhan, hanya yang berhak yang dapat mengubah data. Perubahan meliputi penulisan, pengubahan, perubahan status, penghapusan dan membuat yang baru.
- Tersedia, data tersedia untuk pihak yang berhak
- Otentisi, host dapat mengecek data pengguna

1. Ada tiga hal yang dapat membuat jaringan lebih aman, yaitu 1. Kontrol Akses, adalah membatasi user yang dapat menggunakan jaringan. Beberapa metode autentifikasi antara lain Password Authentication Protocol (PAP), Challenge Handshake Protocol (CHAP) dan Extensible Authentication Protocol (EAP).
2. Privasi, melakukan penyembunyian informasi dari orang yang tidak berhak, dengan cara dilakukan proses enkripsi.
3. Authentikasi, adalh proses pemeriksaan peralatan user yang sah, sehingga paket yang dikirim benar-benar berada ditangan yang berhak.

Beberapa resiko keamanan yang mungkin terjadi dalam teknologi wireless antara lain :

- Serangan penyusupan
- *Bypass monitoring* jaringan
- *Jamming* atau *Denial of Service (DoS)*
- Serangan client to client
- *Brute force attacks* pada password-password access point
- Serangan enkripsi
- Miskonfigurasi

3 Metode Keamanan pada Teknologi *WirelessMAN*.

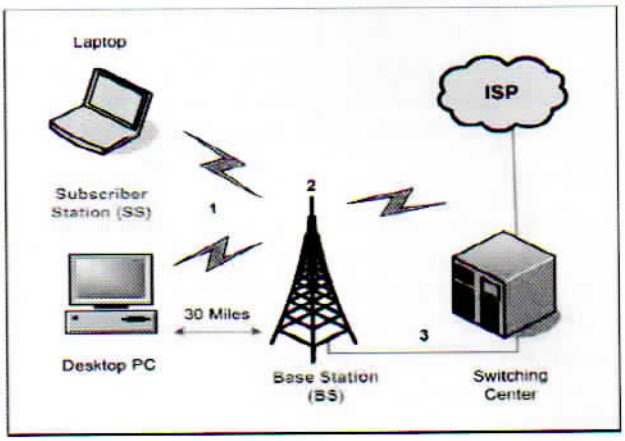
Prinsip kerja *WirelessMAN*

Teknologi *WirelessMAN* (IEEE 802.16/WiMAX) dapat mengkover area sekitar 50 kilometer , dimana ratusan pelanggan akan mentransmisikan data dengan kecepatan sampai 155 Mbps. Dengan demikian faktor keamanan merupakan aspek yang sangat penting bagi pengguna internet yang menggunakan fasilitas ADSL ataupun teknologi kabel modem maupun yang berlangganan dengan teknologi WiMAX.

Sistem pengamanan data dilakukan pada *physical layer* (PHY) dan *data link layer* (MAC) pada suatu arsitektur jaringan, tepatnya pada *base station* (BS) untuk distribusi ke wilayaah sekelilingnya dan subscriber station (SS) untuk komunikasi *point to multiple point*. Sedangkan *Base Station* (BS) dihubungkan secara langsung dengan jaringan publik.

Secara umum trafik WirelessMAN, seperti yang digambarkan pada gb.3.1, terdiri dari tiga bagian :

1) Pelanggan mengirimkan data dengan kecepatan 2-155 Mbps dari SS ke BS
2) BS akan menerima sinyal dari berbagai pelanggan dan mengirimkan pesan melalui udara atau kabel ke switching center melalui protikol IEEE 802.16
3) Switching center akan mengirimkan pesan ke Internet Service Provider (ISP) atau Public Switched Telephone Network (PSTN).



Gambar 2 Trafik yang terjadi pada WiMAX

Pada gambar 2 diatas, laptop atau desktop Personal Computer (PC) berfungsi sebagai SS dan antena tower beserta perangkatnya berfungsi sebagai BS dan switching center yang mengatur pilihan koneksi ke internet service provider.

Dalam teknologi WiMAX, sebuah base station (BS) akan meng-kover seluruh wilayah kota yang terdiri dari ratusan mungkin lebih ribuan pelanggan *(subscriber)*. Semua pelanggan tersebut menggunakan media transmisi yang sama yaitu udara untuk mengirimkan data. Teknologi yang dipakai untuk komunikasi antara *subscriber station* (SS) dengan *base station* (BS) menggunakan teknologi *Time Division Multiple Access* (TDMA).

Ancaman yang umum dihadapi oleh pelanggan berdasarkan teknologi WiMAX adalah :

- Pencurian sinyal atau layanan
- Pencurian data user
- Kloning

Dalam standar IEEE 802.16 digunakan metode keamanan yang berupa *authentification, authorization* dan *encryption.*

Untuk menjamin kerahasiaan data para pelanggan, maka pengirim/penerima data dari SS ke BS dienkripsi menggunakan X.509 yang telah disertifikasi oleh RSA. Dalam standar IEEE 802.16 untuk meningkatkan keamanan dipergunakan aunthetication, authorization dan encryption.

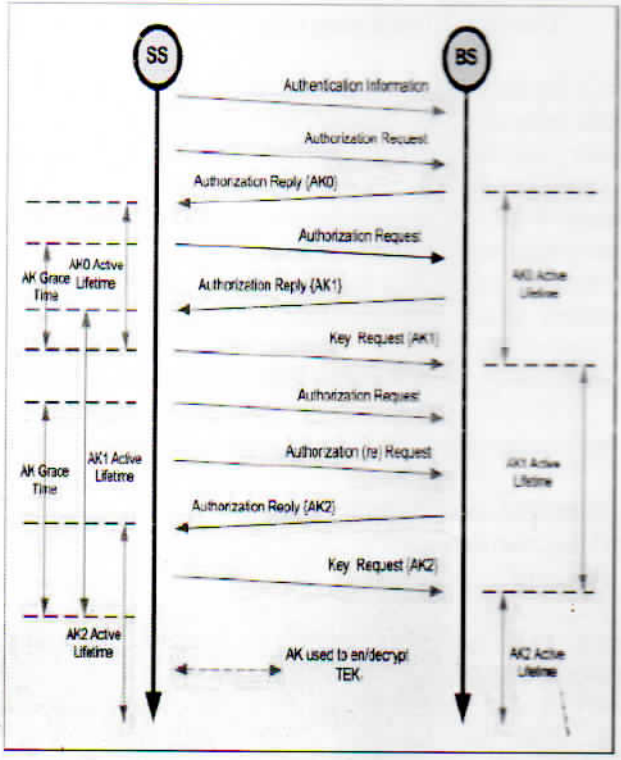
Authentication dan *authorization* pada SS digunakan X.509 dengan kunci publik untuk mengidentifikasi informasi, misalnya UserID, SS'name dan lain sebagainya. Informasi ini akan terus teridentifikasi selama komunikai antara SS dan BS masih berlangsung.

Encryption yang digunakan dalam standar IEEE 802.16 adalah 56 bit DES pada mode Cyclic Block Chaining (CBC). Kesalahan yang terjadi pada *cypertext* tidak dipropagasikan ke dalam *plaintext* dengan menerapkan algoritma *multiple encryption.* Sistem pengamanan data dengan enkripsi antara SS dan BS terletak pada Privasi Sublayer. BS memproteksi pengaksesan data dengan enkripsi pada seluruh jaringan.

Dalam privasi sublayer dibedakan menjadi dua protocol, yaitu :

- Protocol Enkapsulasi bertanggung jawab terhadap data yang melewati jaringan Broadband Wireless Access (BWA).
- Protokol Managemen Kunci Privasi (Privacy Key Management) menyediakan keamanan distribusi antara SS dan BS.

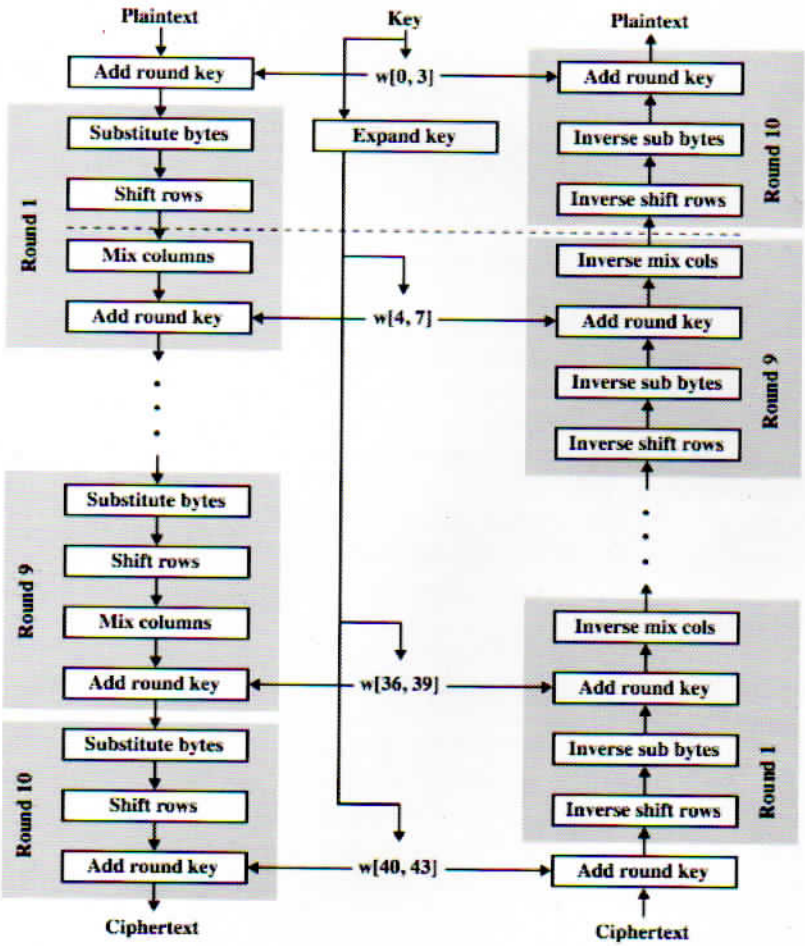
Proses authentication secara lengkap ditunjukkan pada gambar 3 berikut ini.



Gambar 3 Proses authentikasi pada jaringan WiMAX

Enkripsi dari WiMAX

WiMAX meng-enkripsi data menggunakan Advanched Encryption Standarad (AES) dalam model CCM. Jika algoritma enkripsi dikenali dengan deretan kriptografik persamaan SA 0x02, data dalam koneksi yang berasosiasi dengan SA akan menggunakan mode CBC dari algoritma (NIST) Special Publication 800-38c, FIPS-197) Standar Enkripsi Data (DES) US untuk meng-enkripsi alat-alat MAC PDU.



Gambar 4 Struktur AES

4 Analisis Sistem Keamanan pada WiMAX

- Sistem komunikasi yang menggunakan perangkat dengan teknologi IEEE 802.16 (WiMAX) dapat dijamin kemanannya apabila :
- *Device authentication*, berkaitan dengan metode untuk menyatakan bahwa informasinya betul-betul asli atau seseorang yang mengakses atau memberikan informasi adalah orang yang dimaksud. Untuk authentication ini digunakan X.509. Digital passports dapat menjamin identifikasi perangkat IEEE 802.16 seperti nirkawat yang digunakan dalam access point.

- Data *confidentiality*, adalah usaha untuk menjaga informasi dari pihak lain yang tidak berhak mengakses. *Confidentiality* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu, sedangkan privacy lebih kearah data-data yang bersifat privat.
- Data Integritas, adalah jaminan terhadap keutuhan data , dapat dilakukan dengan digital signature atau hash function.

Untuk mencapai tingkat keamanan dan efisiensi yang tinggi, teknologi WiMAX sebaiknya menggunakan :

- 128 bit A*dvanced Encryption Standard* (AES) untuk kecepatan dan enkripsi simetrik untuk menjaga confidentiality
- HMAC-SHA-1 untuk kecepatan dan keutuhan data.
- 256-bit ECMQV untuk kecepatan dan keamanan data, autentikasi dan transport menggunakan 128-bit AES.

WiMAX mampu melayani pelanggan dalam area yang luas yaitu maksimum 50 km dengan kompatibilitas yang tinggi
Memiliki fitur yang lebih banyak dibandingkakan dengan WiFi, dimana standard IEEE 802.16 digabungkan dengan ETSI HiperMAN.
WiMAX tidak hanya dapat melayani para pengguna dengan antenna tetap saja, tetapi juga dapat melayani perangkat yang mobile.
Daerah spektrum frekuensi teknologi WiMAX termasuk lebar, dengan didukung pengaturan kanal yang fleksibel, maka pengguna masih tetap dapat terhubung dengan BTS selama mereka berada dalam daerah operasi BTS.
WiMAX juga memberikan fasilitas *Quality of Service* (QoS).

5 Kesimpulan dan Saran

Dari analisis mengenai sistem keamanan pada WiMAX dapat diambil beberapa kesimpulkan sebagai berikut :

- Sistem keamanan WiMAX cukup baik, unik dan hanadal, oleh karena menggunakan advanced encryption standard (AES) 128 bit, 192 bit dan 256 bit. Sedangkan WiFi hanya menggunakan enkripsi later 64 bit.
- Oleh karena teknologi WiMAX mempunyai kelebihan bila dibandingkan dengan WiFi dalam ber internet, maka sebaiknya dilakukan penelitian lebih lanjut .

6 Daftar Pustaka

[1] Early, Aaron A., 2006, *Wireless Security Handbook*
[2] Siyamta, *Sistem keamanan pada IEEE 802.16/Worldwide Inter-operability for Microwave Access*
[3] Stallings William, *Network Security Data and Computer Communications*
[4] Smith Clint and Meyer John, *3G Wireless with WiMAX and Wi-Fi, Mc Graw Hill*, New York, 2005
[5] Rittinghouse and Ransoms James, *Wireless Operational Security*, 2004
[6] Nuaymi, Loutfi; *WiMAX Technology for Broadband Wireless Access*, John Wiley & Sons, 2007