ARSITEKTUR, KEAMANAN DAN PASAR WIMAX

Helmi Kurniawan[1)], Reza Pulungan [2)]
[1]*Program Studi Teknik Informatika STMIK Potensi Utama*
[2]*Jurusan Ilmu Komputer dan Elektronika, Universitas Gadjah Mada, Yogyakarta*
E-mail: helmikk12@gmail.com, pulungan@ugm.ac.id

Abstrak
WiMAX (Worldwide Interoperabilitas untuk Microwave Access) adalah standar IEEE 802.16 Broadband Wireless Access (BWA). Ini adalah revolusi terbaru dalam teknologi BWA yang telah menarik perhatian banyak kalangan industri nirkabel. Keuntungan utama dari WiMAX adalah kemampuannya untuk menyediakan akses broadband ke daerah-daerah di mana sulit memiliki infrastruktur kabel. WiMAX menawarkan akses broadband yang fleksibel biaya efektif dan efisien. IEEE 802.16-2004 standar diumumkan September 2004 berfokus pada BWA tetap. Banyak industri telah meluncurkan produk mereka berdasarkan standar ini. Namun, berbagai kerentanan keamanan telah ditemukan dalam standar yang mengarah ke berbagai intrusi. Sebuah banyak meratifikasi standar IEEE 802.16e juga dikenal sebagai Mobile WiMAX telah diterbitkan untuk mengatasi masalah ini tetapi perangkat belum dirilis. Makalah ini menggambarkan ikhtisar WiMAX, menguraikan komponen arsitektur fundamental untuk WiMAX dan menjelaskan Masalah Keamanan WiMAX. Selanjutnya berbagai arsitektur protokol standar 802.16, IEEE 802.16 dan Pasar WiMAX.

Kata Kunci: WIMAX; IEEE 802.16; Keamanan; Protocol; Pasar;

1. PENDAHULUAN

WiMAX, yang berarti Worldwide Interoperabilitas untuk Microwave Access, adalah teknologi telekomunikasi nirkabel yang menyediakan transmisi data menggunakan berbagai mode transmisi, dari link point-to-multipoint untuk akses internet sepenuhnya portabel dan mobile. Teknologi yang menyediakan sampai dengan 10 Mbps kecepatan broadband tanpa membutuhkan kabel. Teknologi ini didasarkan pada standar IEEE 802.16 (juga disebut Broadband Wireless Access). Nama "WiMAX" diciptakan oleh Forum WiMAX, yang dibentuk pada bulan Juni 2001 untuk meningkatkan kesesuaian dan interoperabilitas dari standar.

Makalah ini menggambarkan WiMAX sebagai "sebuah standar teknologi yang memungkinkan pengiriman akses broadband wireless last mile sebagai alternatif kabel dan DSL" [1]. Sebagai dibandingkan dengan teknologi nirkabel seperti Wi-Fi, WiMAX lebih kebal terhadap gangguan, memungkinkan penggunaan bandwidth yang lebih efisien dan dimaksudkan untuk memungkinkan kecepatan data yang lebih tinggi jarak yang lebih jauh. Karena beroperasi pada spektrum berlisensi, selain frekuensi tanpa izin, WiMAX menyediakan lingkungan diatur dan model ekonomi yang layak untuk operator nirkabel. Manfaat ini, ditambah dengan dukungan global teknologi (misalnya, penyebaran di seluruh dunia yang sedang berlangsung, alokasi spektrum dan standardisasi), menjadikannya pilihan populer untuk pengiriman cepat dan hemat biaya akses broadband super cepat nirkabel untuk wilayah terlayani di seluruh dunia [2] . WIMAX lebih murah dibanding DSL kabel karena tidak memerlukan menempatkan kabel di sekitar area yang akan dihubungkan, yang merupakan investasi besar bagi provider. Tidak memerlukan investasi ini membuka pintu banyak penyedia layanan yang dapat memulai keluar ritel broadband nirkabel dengan modal rendah, sehingga menyebabkan harga turun karena persaingan. Seperti halnya teknologi nirkabel, persyaratan untuk WiMAX pada dasarnya pemancar dan penerima. Pemancar adalah menara WiMAX, mirip sebuah menara GSM. Itu adalah bagian dari fasilitas operator selular. Satu menara, juga disebut base station, dapat menyediakan cakupan ke suatu daerah dalam radius sekitar 50 km. Di sisi lain, untuk menerima gelombang WiMAX, dibutuhkan penerima untuk WiMAX untuk menghubungkan komputer atau perangkat.

WiMAX memiliki lingkaran jangkauan sekitar 50 km. Medan, cuaca dan bangunan mempengaruhi rentang dan ini sering menyebabkan banyak orang yang tidak menerima sinyal cukup baik untuk koneksi yang tepat. Orientasi juga masalah, dan beberapa orang harus memilih untuk menempatkan modem WiMAX di dekat jendela dan berbalik arah spesifik tertentu untuk penerimaan yang baik. Sambungan WiMAX biasanya non-line-of-sight, yang berarti bahwa pemancar dan penerima tidak perlu memiliki garis yang jelas antara mereka. Tapi versi line-of-sight ada, di mana kinerja dan stabilitas jauh lebih baik, karena ini tidak jauh dengan masalah yang terkait dengan medan dan bangunan [3].

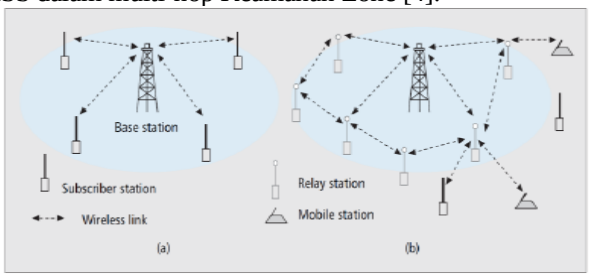
2.ARSITEKTUR KOMPONEN DASAR WIMAX

WiMAX memiliki empat komponen arsitektur fundamental:

1. Base Station (BS). BS adalah node yang logis menghubungkan perangkat pelanggan nirkabel ke jaringan operator. BS memelihara komunikasi dengan perangkat pelanggan dan mengatur akses ke jaringan operator. Sebuah BS terdiri dari unsur-unsur infrastruktur yang dibutuhkan untuk memungkinkan komunikasi nirkabel, yaitu, antena, transceiver, dan peralatan lainnya transmisi gelombang elektromagnetik. BSS biasanya tetap

node, tetapi mereka juga dapat digunakan sebagai bagian dari solusi mobile-misalnya, mungkin BS diletakkan pada kendaraan untuk menyediakan komunikasi untuk perangkat WiMAX di dekatnya. Sebuah BS juga berfungsi sebagai Master Relay-Base Station di relay topologi multi-hop.

2. Subscriber Station (SS). SS adalah sebuah node nirkabel tetap. Sebuah SS biasanya berkomunikasi hanya dengan BSS, kecuali untuk operasi multi-hop jaringan relay. SSS tersedia di kedua model outdoor dan indoor.
3. Mobile Subscriber (MS). Didefinisikan dalam IEEE 802.16e-2005, MSS adalah node wireless yang bekerja pada kecepatan kendaraan dan mendukung mode manajemen daya yang disempurnakan operasi. Perangkat MS biasanya kecil dan self-powered, misalnya, laptop, telepon selular, dan perangkat elektronik portabel.
4. Relay Station (RS). Ditetapkan di 802.16j IEEE-2009, RSS SSS dikonfigurasi untuk meneruskan lalu lintas ke RSS lain, SSS, atau MSS dalam multi-hop Keamanan Zone [4].



Gambar 1. Jaringan WiMAX arsitektur: (a) mode PMP, (b) mesh mode [5].
Sumber: *David Johnston & Jesse Walker,2009, IEEE 802.16 security*

Perangkat WiMAX berkomunikasi menggunakan dua jenis pesan: pesan manajemen dan pesan data. Pesan data transportasi data di seluruh jaringan WiMAX. Pesan Manajemen digunakan untuk menjaga komunikasi antara SS / MS dan BS, yaitu, mendirikan parameter komunikasi, pertukaran pengaturan keamanan, dan melakukan pendaftaran kejadian sistem (jaringan entri awal, handoffs, dan lain-lain) IEEE 802.16 mendefinisikan pita frekuensi untuk operasi WiMAX berdasarkan tipe sinyal propagasi. Dalam satu jenis, WiMAX menggunakan frekuensi radio (RF) balok untuk menyebarkan sinyal antara node. Perbanyakan atas balok ini sangat sensitif terhadap hambatan RF, sehingga pandangan terhalang antara node yang diperlukan. Jenis propagasi sinyal, disebut line of sight (LOS), terbatas pada operasi tetap dan menggunakan 10-66 gigahertz (GHz) rentang frekuensi. Jenis lain dari propagasi sinyal disebut non-line-of-sight (NLOS). NLOS menggunakan teknik modulasi RF canggih untuk mengimbangi perubahan sinyal RF yang disebabkan oleh hambatan yang akan mencegah komunikasi LOS. NLOS dapat digunakan untuk kedua operasi WiMAX tetap (dalam kisaran 2-11 GHz) dan operasi mobile (dalam kisaran 2-6 GHz). NLOS propagasi sinyal lebih umum digunakan daripada LOS karena kendala yang mengganggu komunikasi LOS dan karena peraturan yang ketat untuk perizinan frekuensi dan penyebaran antena di banyak lingkungan yang menghambat kelayakan dari penggunaan LOS [4].

3. IEEE 802.16

IEEE 802.16 dalam mengembangkan versi pertama untuk mengatasi garis pandang (LOS) akses pada rentang spektrum dari 10 GHz sampai 66 GHz. Teknologi ini telah berkembang melalui beberapa update dengan standar tersebut, seperti 802.16a 802.16c, Tetap WiMAX 802.16d (802.16-2004) spesifikasi dan terakhir mengatur mobile 802.16e yang saat ini tersedia secara komersial. 802.16m mendatang masih jauh dari ratifikasi. Update pertama menambahkan dukungan untuk 2 GHz melalui spektrum 11 GHz dengan kemampuan NLOS. Setiap update menambahkan fungsionalitas tambahan atau memperluas jangkauan standar. Misalnya, revisi 802.16c menambahkan dukungan untuk rentang spektrum baik berlisensi dan tidak berlisensi dari 2 GHz sampai 10 GHz. Hal ini juga meningkatkan kualitas layanan (QOS) dan perbaikan tertentu dalam kontrol akses media (MAC) lapisan bersama dengan menambahkan dukungan untuk standar HiperMAN Eropa. Jumlah didukung lapisan fisik (PHY) meningkat. Transportasi media seperti IP, Ethernet dan modus transfer asinkron (ATM) ditambahkan.

Pada intinya, teknologi ini dimaksudkan untuk mengambil sejumlah perangkat tambahan kepemilikan terbaik bibit yang telah dibuat oleh vendor menggunakan standar 802.11 dan menggabungkan mereka bersama-sama dalam produk WiMAX yang sangat berharga dan standar. Sebagai contoh, teknologi nirkabel broadband yang lebih tua seperti Wi-Fi atau 802.11b sistem digunakan operator akses beberapa dengan deteksi tumbukan (CSMA / CD) metode crosstalk untuk base station dan pelanggan tetap premis (CPE) untuk berbicara satu sama lain. Pada dasarnya, ini berarti bahwa setiap radio selalu berbicara dan menciptakan overhead tidak efisien. Hal ini juga mengakibatkan, terutama pada saat-saat lalu lintas yang tinggi, dalam tabrakan paket meningkat dan transmisi ulang, lebih memperburuk masalah. Beberapa sistem berpemilik MAC dibangun kemudian memanfaatkan stasiun pangkalan untuk menentukan kapan CPE akan disurvei dalam rangka untuk menghilangkan masalah ini. Dalam cara penyembuhan permanen protokol 802.16 mendukung beberapa metode pemungutan suara yang vendor dapat memilih untuk menggunakan. Beberapa di antaranya adalah permintaan

polling overhead membonceng dalam lalu lintas, pemungutan suara kelompok atau dinamis mengoptimasi bandwidth dari unit lain oleh CPE. Kuncinya adalah bahwa radio akan dipertukarkan berdasarkan profil produk awal Forum dan juga lebih efisien [6].

A. Berbagai Standar 802.16

802.16a: Izin Frekuensi 2 GHz sampai 11 GHz. Kerja IEEE 802.16a beroperasi pada spesifikasi MAC dan PHY dan menentukan pengalihan koneksi non-visual (NLOS). Frekuensi yang penting bagi 3,5 GHz dan 5,8 GHz untuk aplikasi berlisensi bebas royalti. Data tersebut berada pada saluran lebar 20 MHz 75 Mbit / s. 802.16a diganti oleh 802.16-2004.

Tabel1 berikut memberikan ringkasan IEEE Keluarga 802.16 standar [8].

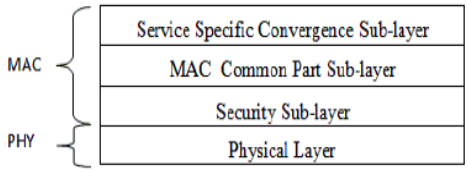
Tabel 1. Keluarga 802.16 Standar

Standard	802.16	802.16a/802.16REVd	802.16e
Spectrum	10 – 66 GHz	<11GHz	<6GHz
Channel Conditions	Line-of-Sight only	None- Line-of-Sight	None- Line-of-Sight
Speed (bit rate)	32 – 34 Mbps	75 Mbps max, 20-MHz channellization	15 Mbps max, 5-MHz channellization
Modulation	QPSK 16QAM 64QAM	OFDM 256 subcarrier QPSK 16QAM 64QAM	Same as 802.16a
Mobility	Fixed	Fixed	Pedestrian Mobility, regional roaming
Channel Bandwidths	20, 25 dan 28 MHz	Selectable Between 1.25 and 25 MHz	Same as 802.6a with sub-channels
Typical Cell Radius	1-3 miles	3-5 miles (up to 30 miles, depending on tower height, antenna gain and transmit power).	1-3 miles

Sumber: *A survey of WiMAX security threats, Trung Nguyen, 2009*

B. Arsitektur protokol IEEE 802.16

Arsitektur protokol IEEE 802.16 ini disusun menjadi dua lapisan utama: Medium Access Control (MAC) layer dan Fisik (PHY) lapisan, seperti yang dijelaskan pada tabel berikut [9]:



Gambar 2. Struktur Protokol IEEE 802.16

Sumber:http://www1.cse.wustl.edu/~jain/cse574-08/ftp/j_bman/sld011.htm

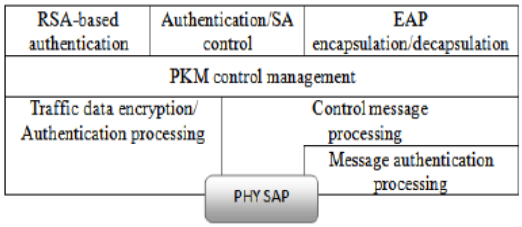
Lapisan MAC terdiri dari tiga lapisan sub. Sub-lapisan pertama adalah Layanan khusus Convergence Sub-layer (CS), yang memetakan data tingkat tinggi pelayanan kepada alur pelayanan lapisan MAC dan koneksi [10]. Sub-lapisan kedua Common Bagian sublayer (CPS), yang merupakan inti dari standar dan terintegrasi dengan sub lapisan keamanan. Lapisan ini mendefinisikan aturan dan mekanisme untuk mengakses sistem, alokasi bandwidth, dan manajemen koneksi. Protokol Data MAC unit dibangun di atas lapisan-sub. Sub terakhir-lapisan dari lapisan MAC adalah Keamanan Sub-layer yang terletak antara CPS MAC dan lapisan PHY, menangani otentikasi, pendirian dan pertukaran kunci, enkripsi dan dekripsi data dipertukarkan antara lapisan MAC dan PHY. Lapisan PHY menyediakan pemetaan dua-arah antara unit-unit data protokol MAC dan PHY layer frame yang diterima dan dikirim melalui coding dan modulasi frekuensi sinyal radio [8].

4. KEAMANAN WIMAX

Menyadari titik mencuat bahwa keamanan telah di adopsi luas layanan broadband wireless, IEEE dan Forum keduanya bertekad untuk menentukan keamanan lingkungan yang kuat. Keamanan WiMAX mendukung dua standar mutu enkripsi, bahwa dari DES3 dan AES, yang dianggap mutakhir. Standar ini mendefinisikan prosesor keamanan khusus pada papan base station untuk starter. Ada juga persyaratan minimum untuk enkripsi lalu lintas dan ujung ke ujung otentikasi yang terakhir yang disesuaikan dari spesifikasi layanan antarmuka data-over-kabel (DOCSIS) BPI + protokol pengamanan. Pada dasarnya, semua lalu lintas pada jaringan WiMAX harus dienkripsi menggunakan Counter Mode dengan mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) yang menggunakan AES untuk keamanan transmisi dan otentikasi integritas data. Akhir untuk otentikasi-akhir PKM-EAP (Protokol Otentikasi yang Diperluas) metodologi yang digunakan yang bergantung pada standar TLS enkripsi kunci publik. Setidaknya satu perusahaan chip prosesor yang dirancang untuk mendukung prosesor onboard standar keamanan [11].

A. Solusi Keamanan WiMAX

Dengan memakai teknologi yang terbaik yang tersedia saat ini, WiMAX, berdasarkan pada standar IEEE 802.16e, memberikan dukungan kuat untuk otentikasi, manajemen kunci, enkripsi dan dekripsi, DNS dan manajemen perlindungan teks biasa dan optimasi protokol pengamanan. Dalam WiMAX, sebagian besar masalah keamanan dibahas dan ditangani di lapisan sub keamanan MAC-seperti yang dijelaskan dalam gambar berikut:

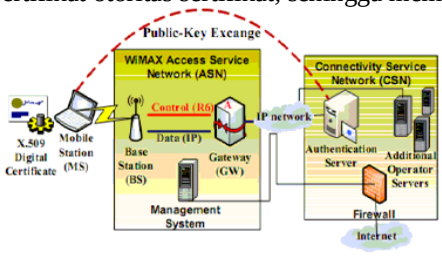


Gambar 3. MAC Keamanan sub-layer.
Sumber: IEEE Std. 802.16e 2006.

Dua entitas utama dalam WiMAX, termasuk Base Station (BS) dan Subscriber Station (SS), dilindungi oleh keamanan WiMAX Berikut adalah beberapa fitur [8]:

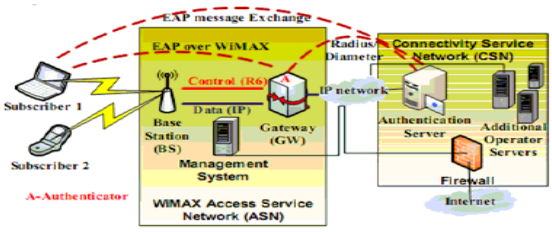
1. Asosiasi keamanan: Sebuah asosiasi keamanan (SA) adalah satu set parameter keamanan informasi bahwa BS dan satu atau lebih dari saham SSS klien dalam rangka mendukung komunikasi yang aman. Data SA memiliki SA 16bit identifier, sebuah (modus DES dalam KBK) Cipher untuk melindungi data selama pengiriman melalui saluran dan dua kunci enkripsi lalu lintas (Teks) untuk mengenkripsi data: satu adalah kunci operasional saat ini dan yang lainnya TEK [12]. Ketika tombol saat ini berakhir, TEK sebuah kunci pengenal 2bit digunakan. Sebuah vektor inisialisasi 64bit (IV) digunakan untuk setiap TEK [13].
2. Infrastruktur kunci publik (PKI): Standar WiMAX menggunakan Privasi dan Key Management Protocol untuk aman mentransfer bahan keying antara base station dan mobile station. Manajemen kunci yang privasi (PKM) protokol bertanggung jawab untuk privasi, manajemen kunci, dan otorisasi sebuah SS ke BS. Draft awal untuk WiMAX mandat penggunaan PKMv1 [14], yang merupakan metode otentikasi satu arah. PKMv1 hanya memerlukan SS untuk otentikasi diri pada BS, yang menimbulkan risiko serangan (MITM) Man-in-the-Middle. Untuk mengatasi masalah ini, PKMv2 diusulkan (kemudian diadopsi oleh 802.16e), yang menggunakan protokol (dua arah) otentikasi timbal balik [15]. Di sini, baik SS dan BS yang diperlukan untuk mengesahkan dan mengotentikasi satu sama lain. PKMv2 adalah mencegah dari yang berikut [16]: BS dan menirukan SS, MITM menyerang dan masalah pertukaran kunci.

   PKMv2 mendukung penggunaan Rivest-Shamir-Adlerman (RSA) nilai tukar kriptografi kunci publik. Pertukaran RSA kunci publik mensyaratkan bahwa stasiun bergerak menentukan identitas baik menggunakan sertifikat X.509 produsen-dikeluarkan digital atau mandat yang dikeluarkan operator seperti modul identitas pelanggan (SIM). Sertifikat X.509 digital berisi stasiun mobile Public-Key (PK) serta alamat MAC. Stasiun bergerak transfer sertifikat X.509 digital untuk jaringan WiMAX, yang kemudian diajukan ke sertifikat otoritas sertifikat. Memvalidasi sertifikat otoritas sertifikat, sehingga memvalidasi identitas pengguna.



Gambar 4. Infrastruktur Kunci Publik [13].
Sumber : *Popovski,2008,IEEE 802.16Security Issues: A Survey*

   Setelah identitas pengguna divalidasi, jaringan WiMAX menggunakan kunci publik untuk membuat kunci otorisasi, dan mengirimkan otorisasi kunci untuk stasiun bergerak. Stasiun bergerak dan base station menggunakan otorisasi kunci untuk mendapatkan kunci enkripsi yang digunakan identik dengan standar enkripsi yang canggih (AES) algoritma [13].
3. Otentikasi: Otentikasi adalah proses untuk memvalidasi identitas pengguna dan seringkali mencakup validasi yang dapat mengakses layanan pengguna. Proses otentikasi biasanya melibatkan pemohon (yang berada di stasiun mobile), sebuah authenticator (yang mungkin berada di base station atau gateway), dan sebuah server otentikasi [13].



Gambar 5. Otentikasi EAP-based [13].
Sumber : *Popovski,2008,IEEE 802.16Security Issues: A Survey*

WiMAX menggunakan Extensible Authentication Protocol (EAP) untuk melakukan otentikasi pengguna dan kontrol akses. EAP sebenarnya merupakan kerangka kerja otentikasi yang membutuhkan penggunaan "metode EAP"untuk melakukan pekerjaan otentikasi yang sebenarnya. Operator jaringan dapat memilih metode EAP seperti EAP-TLS (Transport Layer Security), atau EAP-TTLS MSCHAP v2 (terowongan TLS dengan versi Microsoft Challenge-Handshake Authentication Protokol 2). Pesan yang didefinisikan oleh metode EAP yang dikirim dari sebuah stasiun mobile authenticator. Authenticator kemudian meneruskan pesan ke server otentikasi baik menggunakan RADIUS atau protokol DIAMETER [17].

4. Privasi dan integritas data: WiMAX menggunakan AES untuk menghasilkan chipertext. AES mengambil kunci enkripsi dan kontra sebagai input untuk menghasilkan sebuah bitstream. Bitstream tersebut kemudian XOR dengan plaintext untuk menghasilkan ciphertext. Algoritma AES merupakan rekomendasi 802.16e lapisan sub-keamanan, karena dapat melakukan perlindungan yang lebih kuat dari pencurian layanan dan data melalui jaringan mobile broadband nirkabel. Selain CCMMode dan ECB-Mode algoritma AES didukung dalam 802.16-2004, 802.16e mendukung tiga lebih algoritma AES: CBCMode AES, RKT-Mode AES dan AES-Key-Wrap [13].

B. Ancaman WiMAX

Meskipun niat baik untuk keamanan WiMAX, ada beberapa potensi serangan terbuka untuk lawan, termasuk:

1. Rogue base station, Serangan DoS, Man-in-the-Middle Attacks
2. Jaringan manipulasi dengan frame manajemen palsu

Tes yang sesungguhnya keamanan WiMAX akan datang ketika penyedia mulai penyebaran skala jaringan yang luas, dan peneliti dan penyerang memiliki akses ke peralatan komoditas CPE. Serangan lain termasuk fuzzing protokol WiMAX dapat memungkinkan penyerang untuk lebih lanjut memanipulasi BSS atau SSS. Sampai saat itu, keamanan WiMAX terbatas untuk spekulasi [18].

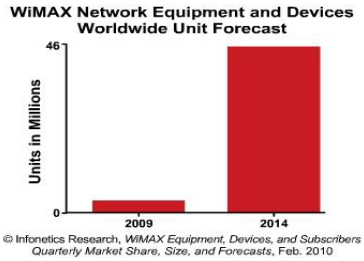
5. PASAR GLOBAL WIMAX

Dunia Interoperabilitas untuk Microwave Access atau WiMAX, telah mendapatkan banyak perhatian sebagai alternatif broadband nirkabel, karena menyediakan akses broadband yang handal, aman dan berkualitas tinggi bagi pengguna internet mobile. Teknologi ini mendukung aplikasi bandwidth-berat dan User Generated Content (UGC) jasa yang pelanggan inginkan. WiMAX menjanjikan alternatif, berperforma lebih baik yang lebih murah untuk teknologi banyak (seperti DSL, Wi-Fi) yang sudah tersedia di pasar. Menurut penelitian baru laporan- Analisis Pasar Global WiMAX, WiMAX memiliki potensi yang luar biasa untuk menawarkan platform standar global broadband nirkabel. Banyak negara di seluruh dunia akan mengadopsi WiMAX untuk memfasilitasi perkembangan ekonomi yang pesat. Selain itu, pindah ke WiMAX, sebuah teknologi yang siap untuk penyebaran sekarang, akan lebih baik untuk menunggu teknologi alternatif yang mungkin tidak tersedia selama tiga tahun atau lebih. Akibatnya, jumlah pengguna WiMAX diperkirakan tumbuh lebih dari 87% antara tahun 2010 dan 2012.

Penelitian ini mengungkapkan bahwa, pada 2012 kawasan Asia-Pasifik akan memimpin jumlah pengguna WiMAX global akuntansi selama lebih dari 45% dari total basis pengguna, diikuti oleh Amerika Utara dan Eropa. Mayor pertumbuhan diperkirakan di Asia-Pasifik dan MEA sebagai negara-negara tersebut menggelar teknologi lebih cepat. Selain itu, dukungan pemerintah dan inisiatif operator untuk menyediakan wilayah dengan akses internet cepat di daerah terpencil juga mendorong pertumbuhan ke pasar WiMAX [19]. Pasar WiMAX keluar dari masa resesi kuat, posting tiga perempat berturut-turut pertumbuhan pendapatan untuk peralatan 802.16e dan perangkat. Dengan Clearwire di AS mengumumkan hasil kuartalan yang kuat, Yota di Rusia berkembang dengan cepat, dan lain-lain seperti UQ di Jepang menjadi agresif, model bisnis WiMAX tampaknya akan bekembang. Meskipun masih awal, WiMAX ini membuktikan menjadi cocok dalam berbagai segmen pasar broadband serta maju berkembang [20].

PASAR UTAMA WIMAX

1. Worldwide vendor pendapatan dari 802.16d dan 802.16e WiMAX peralatan jaringan dan perangkat mencapai $ 1080000000 pada tahun 2009, turun 19% dari tahun 2008, karena pasar mengalami dampak resesi
2. Namun, 4Q09 adalah kuartal berturut-turut ketiga peralatan perangkat WiMAX dan pertumbuhan pendapatan, naik 3% dari 3Q09
3. Tingkat pendapatan Triwulanan tetap rendah dari tertinggi presesi pasar lebih dari $ 300,000,000 terlihat pada awal 2008
4. Pasar WiMAX menunjukkan tanda-tanda positif pertumbuhan stabil dari tahun ini dan seterusnya, dengan berlangsung penggelaran besar di Amerika Serikat, Jepang, Rusia, dan India
5. Mulai tahun 2011-2012, 802.16m WiMAX produk diharapkan untuk diuji, bersertifikat, dan tersedia secara komersial, menawarkan kecepatan sebanding dengan LTE
6. Untuk peralatan WiMAX gabungan dan pasar perangkat, Motorola mengambil tempat # 1 pada tahun 2009, dengan 17% dari pendapatan di seluruh dunia, tepat di depan Alvarion
7. Huawei menunjukkan pertumbuhan terbesar dalam peralatan WiMAX dan berbagi perangkat pasar di tahun 2009
8. Jumlah pelanggan WiMAX melonjak 75% pada tahun 2009-6800000 seluruh dunia [21].



Gambar 6. Pasar WiMAX

6. KESIMPULAN

WiMAX memungkinkan operator untuk menampilkan pelanggan mereka konektivitas broadband di sepenuhnya mobile, semua jaringan IP. Standar IEEE 802.16e telah mengubah beberapa mekanisme keamanan dan memerlukan penelitian lebih lanjut tentang efek kerentanan. WiMAX adalah teknologi yang sangat menjanjikan untuk pengiriman layanan broadband mobile sepenuhnya pribadi. Pasar WiMAX menyajikan peluang bisnis yang sangat besar. WiMAX dapat digunakan untuk mendorong aliran pendapatan baru pada garis waktu lebih pendek dan pada kabel jauh lebih rendah daripada FTTx, xDSL, atau alternatif kabel modem. WiMAX adalah sebuah kesempatan.

DAFTAR PUSTAKA

1. *WiMax Forum - Technology*. http://www.wimaxforum.org/technology *2008-07-22.*
2. http://www.agilent.com/about/newsroom/tmnews/background/wimax/. *2009-11-18.*
3. *Nadeem Unuth,* http://voip.about.com/od/mobilevoia/UsingWiMAXTechnology.htm. *2009-10-12.*
4. *Karen Scarfone, Cyrus Tibbs, Matthew Sexton, 2009,Guide to Security for WiMAX Technologies, US National Institute of Standards and Technology-Special Publication 800-127(Draft), 46 pages (Sep. 2009)*
5. *David Johnston & Jesse Walker,2009, Overview of IEEE 802.16 security*
6. *http://slingbroadband.com/wimax/category/wimax-faq// . Retrieved 2008-11-28.*
7. *http://www.wifinotes.com/wimax/IEEE-802.16.html*
8. *Trung Nguyen, 2009, A survey of WiMAX security threats, http://www.cse.wustl.edu/~jain/cse571-09/ftp/wimax2/index.html*
9. *http://www.cse.wustl.edu/~jain/cse574-08/*
10. *Department University of Bridgeport, Bridgeport, CT*
11. *http://www.asee.org/activities/organizations/zones/proceedings/zone1/2008/Professional/ASEE12008_0022_paper.pdf*
12. *http://slingbroadband.com/wimax/category/wimax-faq//.2008-11-28.*
13. *J. Hasan, 2006, Security Issues of IEEE 802.16 (WiMAX), School of computer and Information Science, Edith Cowan University, Australia, 2006.*
14. *Mitko Bogdanoski, Pero Latkoski, Aleksandar Risteski, Borislav Popovski,,2008,IEEE 802.16Security Issues: A Survey, Faculty of Electrical Engineering and Information Technologies, Ss. Cyril and Methodius University, Skopje, Macedonia.,http://2008.telfor.rs/files/radovi/02_32.pdf*
15. *D. Johnston and J. Walker, 2004, Overview of IEEE 802.16 Security, IEEE Security & Privacy, magazine May/June 2004.*

16. *S. Adibi, G. B. Agnew,T. Tofigh, 2008,End-to-End (E2E) Security Approach in WiMAX: Security Technical Overview for Corporate Multimedia Applications, 747-758, Handbook of Research on Wireless Security (2 Volumes) Edited By: Yan Zhang, Jun Zheng, Miao Ma, 2008.*
17. *S.Adibi, G. B. Agnew, 2008, End-to-End Security Comparisons Between IEEE 802.16e and 3G Technologies, 364 – 378, Handbook of Research on Wireless Security (2 Volumes) Edited By: Yan Zhang, Jun Zheng, Miao Ma, 2008.*
18. *S. Adibi, G. B. Agnew, 2008, Extensible Authentication (EAP) Protocol Integrations in the Next Generation Cellular Networks, 776-789, Handbook of Research on Wireless Security (2 Volumes) Edited By: Yan Zhang, Jun Zheng, Miao Ma, 2008.*
19. *Joshua W, http://www.computerworld.com.au/article/170510/wimaxsecurityissues/?fp=16&fpid=1, Network World*
20. *Global WiMAX Market Analysis, 2009, http://www.bharatbook.com/Market-Research-Reports/Global-WiMAX-Market-Analysis.html*
21. *Webb Richard, 2010, London, United Kingdom, March 1, 2010—Infonetics Research*
22. *WiMAX Equipment, Devices, and Subscribers market share and forecast report,2010, www.infonetics.com*