Tinjauan Teknis Teknologi Perangkat Wireless dan Standar Keamanannya

Aji Supriyanto
Fakultas Teknologi Informasi, Universitas Stikubank Semarang
e-mail : ajisup@gmail.com

ABSTRAK : Teknologi komunikasi wireless yang banyak berkembang saat ini adalah *Bluetooth*, Wi-Fi, Wi-MAX. Masing-masing memiliki karakteristik yang berlainan meskipun sama-sama menggunakan pita frekwensi tinggi. Teknologi bluetooth menggunakan protokol IEEE 802.15.1, dan Wi-Fi berada di bawah spesifikasi 802.11.Sedangkan WiMAX dikembangkan mulai dari standar 802.16 kemudian berevolusi ke standar 802.16a (direvisi menjadi 802.16d) kemudian yang terakhir adalah 802.16e.

Model penanganan kemanan yang dilakukan pada peangkat komunikasi yang menggunakan frekewensi diatas semestinya mengacu pada standar yang dikeluarkan IEEE yang dinamakan standar IEEE 802.1x yang merupakan standar keamanan jaringan yang mempunyai banyak mekanisme untuk autentifikasi.

Kata kunci : Bluetooth, WiFi, WiMAX, karakteristik, dan standar keamanan

PENDAHULUAN

Teknologi wireless yang terkenal dan banyak digunakan pada laptop, maupun perangkat komunikasi lain seperti PDA, printer, mouse dan *Handphone.* adalah *Bluetooth*, Wi-Fi (*Wireless Fidelity*), Wi-MAX (*Worldwide Interoperability for Microwave Access*). Masing-masing teknologi wireless tersebut memiliki karakteristik sendiri, sehingga perlu adanya penaganan keamanan yang juga tersendiri. Namun begitu karena teknologi yang digunakan adalah sama yaitu wireless selain memiliki karakteristik yang berlainan, maka juga ada beberapa hal sama.

Model penanganan keamanan pada teknologi wireless antara yang satu dnegan yang lain dimungkinkan dapat berlainan, namun pada prinsipnya bahwa standar yang digunakan untuk implementasi keamanan terdapat banyak kesamaan. Untuk itu perlu dijabarkan terlebih dahulu karakteristik masing-masing teknologi wireless, kemudian diimplementasikan keamanannya sesuai dengan standar yang telah ditentukan.

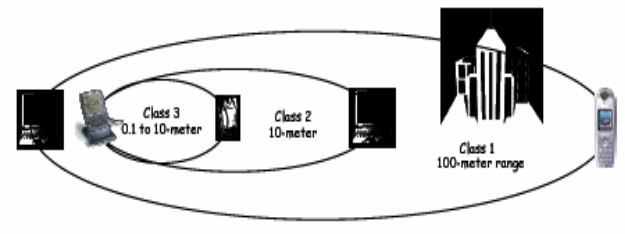
BLUETOOTH

Teknologi bluetooth menggunakan protokol IEEE 802.15.1, dan Wi-Fi berada di bawah spesifikasi 802.11. Kecepatan transfer dan area jangkauan bluetooth dalam transfer data, cocok untuk perangkat-perangkat kecil seperti PDA, karena daya jangkau dan transfernya lebih kecil dibanding Wi-Fi yang memiliki jangkauan lebih luas dan transfer datanya lebih besar. Meskipun begitu Bluetooth memiliki keunggulan dalam transmisi yang dapat dilakukan secara bersamaan dalam dua arah (*full-duplex*) dan biasanya merupakan perangkat yang integral dibanding dengan Wi-Fi yang biasanya diimplementasikan dalam sebuah alat network tersendiri.

Bluetooth adalah sebuah teknologi komunikasi wireless (tanpa kabel) yang beroperasi dalam pita frekuensi 2,4 GHz *unlicensed* ISM (*Industrial, Scientific and Medical*) dengan menggunakan sebuah frequency hopping tranceiver yang mampu menyediakan layanan komunikasi data dan suara secara real-time antara host-host bluetooth dengan jarak jangkauan layanan yang terbatas dan kecepatan dibawah 1 Mbps. Berdasarkan jangkauan operasinya, perangkat Bluetooth dibagi ke dalam tiga kelas yaitu:

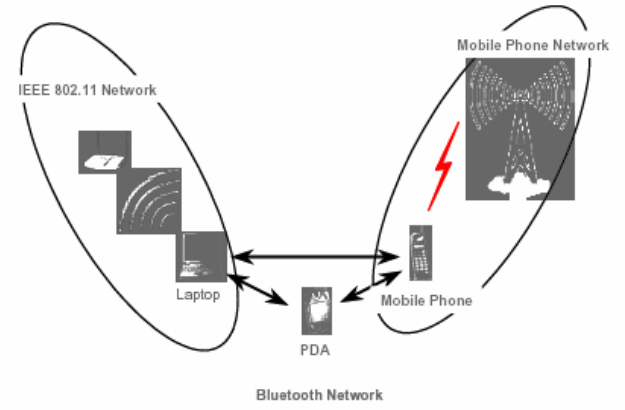
- **Class 3 device.** Perangkat Bluetooth yang mempunyai daya transmisi sebesar 1 mW dan jangkauannya antara 0,1 sampai 10 meter.

- **Class 2 device.** Perangkat Bluetooth yang mempunyai daya transmisi sebesar 1 sampai 2,5 mW dan jangkauannya sekitar 10 meter.
- **Class 1 device.** Perangkat Bluetooth yang mempunyai daya transmisi sebesar 100 mW dan jangkauannya sejauh 100 meter.



Gambar 1. Jangkauan operasi Bluetooth

Pada saat dua perangkat bluetooth melakukan komunikasi, keduanya akan menggunakan protocol LMP (*Link manager Protocol*) untuk mengawali, melakukan otentikasi, mengelola session, dan memanajemen sumber daya yang digunakan. Sedangkan jika komunikasi dilakukan oleh lebih dari dua perangkat dalam satu session, maka dikatakan bahwa alat tersebut tergabung dalam sebuah *piconet*. Piconet adalah sebuah jaringan yang bekerja seperti 802.11b dalam modus Ad-Hoc, dengan perbedaan bahwa salah satu alat akan menjadi *master*, sedangkan alat lain menjadi *slave*, dengan tujuan untuk memelihara agar aliran frekwensi tetap sinkron. Sebanyak 10 *piconet* dapat dikoneksikan untuk membuat *scatternet*, meskipun dianggap sebagai cara yang tidak praktis. Modus komunikasi *Ad-Hoc* adalah modus komunikasi yang dapat dilakukan secra langsung antara satu dengan yang lainnya.



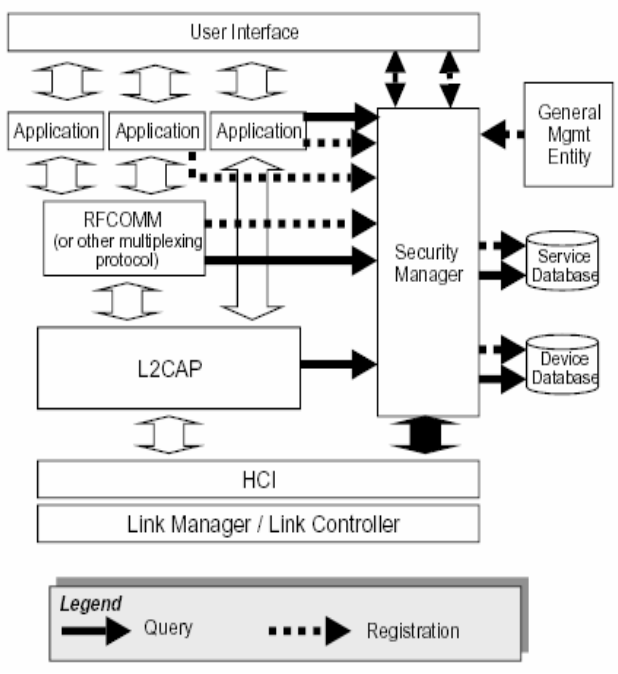
Gambar 2. Modus komunikasi Ad Hoc

Tabel 1. Karakteristik teknologi Bluetooth

Karakteristik	Deskripsi
Physical Layer	Frequency Hopping Spread Spectrum (FHSS)
Frequency Band	2,4 – 2,4835 GHz (ISM band)
Hop Frequency	1.600 hop/detik
Kecepatan data	1 Mbps (raw)
Keamanan Data dan Jaringan	▪ Tiga mode keamanan ▪ Dua tingkat device trust ▪ Tiga tingkat keamanan layanan ▪ Enkripsi stream untuk confidentiality, ▪ Challenge response untuk authentication, ▪ PIN-derived key ▪ Limited management
Jangkauan	Sekitar 10 meter dan dapat diperluas sampai 100 meter
Throughput	~ 720 kbps
Kelebihan	▪ Tanpa kabel, ▪ Sinyal dapat menembus tembok/halangan, ▪ Biaya relatif murah, ▪ Berdaya rendah, dan ▪ Hardware yang relatif kecil.
Kekurangan	▪ Kemungkinan terjadinya interferensi dengan teknologi lain yang menggunakan ISM band, ▪ Kecepatan data relatif rendah, dan ▪ Sinyal yang lemah di luar batasan.

Arsitektur Keamanan Bluetooth

Teknologi Bluetooth menggunakan mekanisme keamanan pada lapisan aplikasi dan lapisan saluran. Selain itu, penggunaan mekanisme seleksi hop sekitar 1.600 hop/detik menghindarkan interferensi dengan piconet atau perangkat ISM lain dan skema pengatur daya keluaran untuk mengatur konsumsi daya pada perangkat mobile sehingga mengurangi jangkauan penyebaran sinyal radio sesuai keperluan transmisi data.



Gambar 3. Arsitektur keamanan Bluetooth

Secara umum, terdapat tiga jenis metode keamanan yang ditetapkan oleh spesifikasi Bluetooth yaitu: otentikasi, kerahasiaan, dan otorisasi.

Security Manager

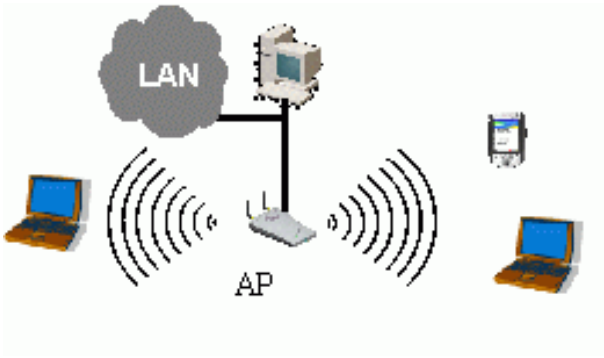
Merupakan suatu komponen Bluetooth yang berfungsi untuk menentukan kebijakan dan fitur-fitur keamanan yang harus diterapkan ketika permintaan suatu hubungan dibuat. Security manager melakukan authentication, enkripsi, dan sebagainya berdasarkan layanan, jenis perangkat, dan tingkat trust perangkat.

Security manager memerlukan informasi berkaitan dengan perangkat dan layanan sebelum mengijinkan akses ke suatu layanan. Informasi tersebut tersimpan di dalam dua database yaitu device database dan service database. Device database menyimpan informasi yang berhubungan dengan jenis perangkat, level trust, panjang link key yang digunakan untuk enkripsi. Service database menyimpan informasi yang berhubungan dengan authentication, authorization, dan enkripsi suatu layanan. Selain itu juga menyimpan informasi ruting untuk layanan.

WI-FI

Wi-Fi memiliki pengertian yaitu sekumpulan standar yang digunakan untuk Jaringan Lokal Nirkabel (Wireless Local Area Networks - WLAN) yang didasari pada spesifikasi IEEE 802.11. Pada WiFi lebih dikenal 3 standar yang popular yaitu 802.11b (paling popular dengan kecepatan data sampai 11 Mbit/sec), 802.11a (54 Mbit/sec dengan jarak lebih kecil dibanding 802.11b) dan 802.11g (kecepatan 54Mbit/sec). Spesifikasi tersebut menawarkan banyak peningkatan mulai dari luas cakupan yang lebih jauh hingga kecepatan transfernya. Frekuensi WiFi hanya bermain pada 2 band yaitu di 2,4 GHz dan 5,8 GHz

Komponen Wi-Fi secara umum terdiri dari AP (*Access Point*) dan *Wireless Client* yang bisa terintegrasi dengan *device* pengguna atau *external card*. AP dapat disambungkan ke jaringan LAN eksisting. Gambar berikut adalah konfigurasi umum WiFi.



Gambar 4. Konfigurasi WiFi

Operasi topologi Wi-Fi memiliki dua modus yaitu *Ad-Hoc* dan *Infrastrucutre*. Ad-Hoc beroperasi secara langsung, seperti yang dilakukan *Bluetooth*, sedangkan modus *Infrastructure* dilakukan melalui satu atau lebih akses point. Akses point merupakan peralatan LAN yang menghubungkan peralatan nirkabel dengan jaringan LAN. Contoh ilustrasinya adalah BTS yang memberi sinyal pada handphone, maka untuk WiFi, contohnya adalah Ethernet. Modus koneksi *Ad-Hoc* adalah mode dimana beberapa komputer terhubung secara langsung, dan salah satu dari komputer - komputer tersebut berfungsi menjadi server dan lainnya menjadi client, atau lebih dikenal dengan

istilah Peer-to-Peer. Keuntungannya, lebih murah dan praktis bila yang terkoneksi cuma 2 atau 3 komputer secara, tanpa harus membeli access point.

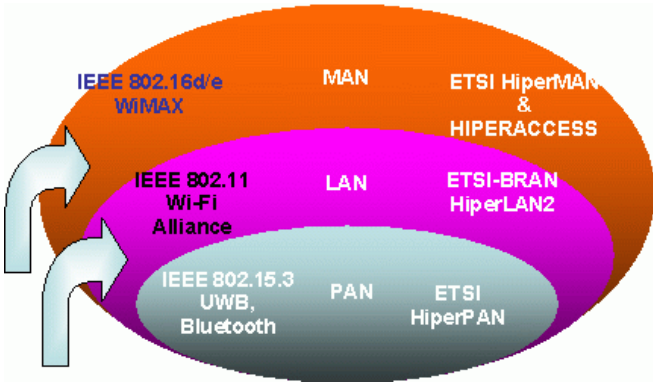
Sedangkan modus *infrastucture* perlu menggunakan Access Point yang berfungsi sebagai pengatur lalu lintas data, sehingga memungkinkan banyak Client dapat terhubung dengan jaringan (Network). Keuntungan dari sistem Wi-Fi , pemakai tidak dibatasi ruang gerak dan hanya dibatasi pada jarang jangkauan dari satu titik pemancar Wi-Fi. Karena sistem Wi-Fi mengunakan transmisi frekuensi secara bebas, maka pancaran signal yang ditransmit pada unit Wi-Fi dapat ditangkap oleh computer lain sesama pemakai Wi-fi. Pada teknologi Wi-Fi ditambahkan juga sistem pengaman misalnya WEP (*Wired Equivalent Privacy*) untuk pengaman sehingga antar computer yang telah memiliki otorisasi dapat saling berbicara.

Keamanan Wi-Fi

Terdapat beberapa jenis pengaturan keamanan jaringan Wi-fi, antara lain: WPA Pre-Shared Key, WPA RADIUS , WPA2 Pre-Shared Key Mixed, WPA2 RADIUS Mixed, RADIUS, WEP.

WiMAX

WiMAX merupakan teknologi nirkabel yang menyediakan hubungan jalur lebar dalam jarak jauh, hingga perkiraan 50 Km. Teknologi ini hampir mirip dengan WiFi ditambah dengan kemampuannya di sisi jarak jangkau, QoS, NLOS *(Non Line of Sight)*, *security* dan berbagai fitur lainnya. Perbandingan jangkauan atau cakupan area (*coverage*) dari *Bluetooth*, Wi-Fi, dan WiMAX dapat dilihat pada gambar dibawah ini.



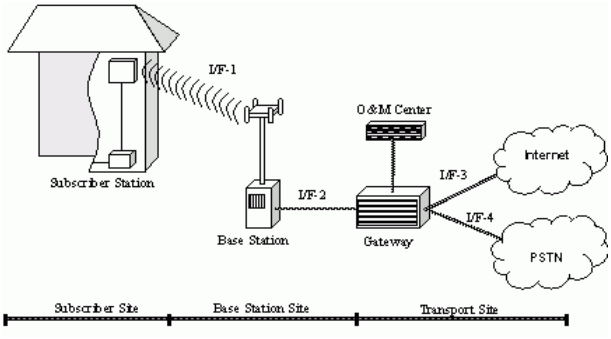
Gambar 5. Deskripsi coverage WiMAX vs WiFi

WiMAX dikembangkan mulai dari standar 802.16 kemudian berevolusi ke standar 802.16a (direvisi menjadi 802.16d) kemudian yang terakhir adalah 802.16e. Standar WiMAX 802.16d dikembangkan untuk melayani pelanggan *fixed* sedangkan 802.16e untuk melayani pelanggan *mobile*.

Tabel 2. Perbandingan Frekuensi WiMAX dan WiFi

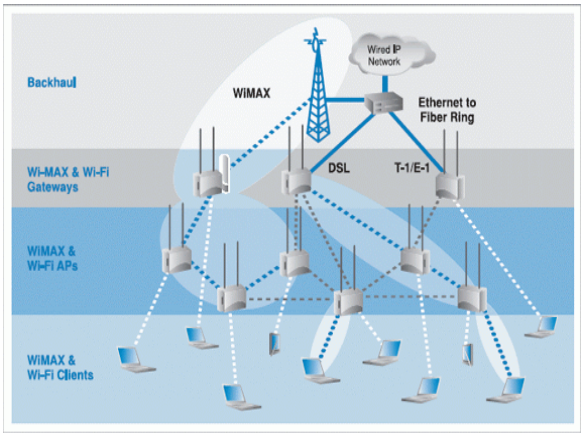
Teknologi	Frekkuensi	Keterangan
WiFi	2,4 & 5,8 GHz	Unlicensed
WiMAX	▪ 2.3 GHz band ▪ 2.5 GHz band ▪ 3.4 – 3.6 GHz band ▪ 5.8 GHz band ▪ Optional : 4.9 – 5.0 GHz ▪ Optional : 700 MHz (in US case) ▪ Optional : 3.3 GHz band	Unlicensed dan licensed

Secara umum komponen WiMAX dibagi menjadi 3 bagian yaitu *subscriber station, base station* dan *transport site*. Untuk *subscriber station* terletak di lingkungan pelanggan (bisa *fixed* atau *mobile/portable*). Sedangkan *base station* biasanya satu lokasi dengan jaringan operator (jaringan IP/internet atau jaringan TDM/PSTN). Untuk memperjelas perhatikanlah gambar 2 yang merupakan konfigurasi generik dari WiMAX.



Gambar 6. Konfigurasi Generik WiMAX

Pemakaian teknologi Wi-MAX dan Wi-Fi secara garis besar keduanya dapat diintegrasikan dan *overlay* (saling melapisi). Kalau integrasi berarti antara WiMAX dan WiFi akan saling mendukung. Keduanya akan saling bersinergi untuk melayani pelanggan yang lebih besar dan lebih banyak. Namun bila sifatnya *overlay* atau *overlap* dari sisi *coverage*, maka dapat difungsikan saling mendukung (bila satu operator) dan juga akan saling berlawanan bila berbeda operator.



Gambar 7. Jaringan Wimax

Keuntungan dan kerugian WiMAX

Banyak keuntungan yang didapatkan dari terciptanya standardisasi industri ini. Para operator telekomunikasi dapat menghemat investasi perangkat, karena kemampuan WiMAX dapat melayani pelanggannya dengan area yang lebih luas dan tingkat kompatibilitas lebih tinggi. Selain itu, pasarnya juga lebih meluas karena WiMAX dapat mengisi *celah broadband* yang selama ini tidak terjangkau oleh teknologi Cable dan DSL (*Digital Subscriber Line*). WiMAX salah satu teknologi memudahkan mereka mendapatkan koneksi Internet yang berkualitas dan melakukan aktivitas. Sementara media wireless selama ini sudah terkenal sebagai media yang paling ekonomis dalam mendapatkan koneksi Internet. Area coverage-nya sejauh 50 km maksimal dan kemampuannya menghantarkan data dengan transfer rate yang tinggi dalam jarak jauh, sehingga memberikan kontribusi sangat besar bagi keberadaan wireless MAN dan dapat menutup semua celah broadband yang ada saat ini. Dari segi kondisi saat proses komunikasinya, teknologi WiMAX dapat melayani para subscriber, baik yang berada dalam posisi Line Of Sight (posisi perangkat-perangkat yang ingin berkomunikasi masih berada dalam jarak pandang yang lurus dan bebas dari penghalang apa pun di depannya) dengan BTS maupun yang tidak memungkinkan untuk itu (Non-Line Of Sight). Jadi di mana pun para penggunanya berada, selama masih masuk dalam area coverage sebuah BTS (Base Transceiver Stations), mereka mungkin masih dapat menikmati koneksi yang dihantarkan oleh BTS tersebut.

Selain itu, dapat melayani baik para pengguna dengan antena tetap (fixed wireless) misalnya di gedung-gedung perkantoran, rumah tinggal, toko-toko, dan sebagainya, maupun yang sering berpindah-pindah tempat atau perangkat mobile lainnya. Mereka bisa merasakan nikmatnya ber-Internet broadband lewat media ini. Sementara range spektrum frekuensi yang tergolong lebar, maka para pengguna tetap dapat terkoneksi dengan BTS selama mereka berada dalam range frekuensi operasi dari BTS. Sistem kerja MAC-nya (Media Access Control) yang ada pada Data Link Layer adalah connection oriented, sehingga memungkinkan penggunanya melakukan komunikasi berbentuk video dan suara.

Kekurangan dari WiMAX antara lain harga peralatan infrastruktur yang masih mahal, kemudian teknologinya masih berkembang terus, sehingga bisa salah investasi, terlalu banyak jenis perangkat yang tidak saling kompatibel karena akibat penyesuaian perkembangan teknologi ini, serta perlu dibutuhkan pengalaman dan keahlian tertentu untuk memasang perangkatnya.

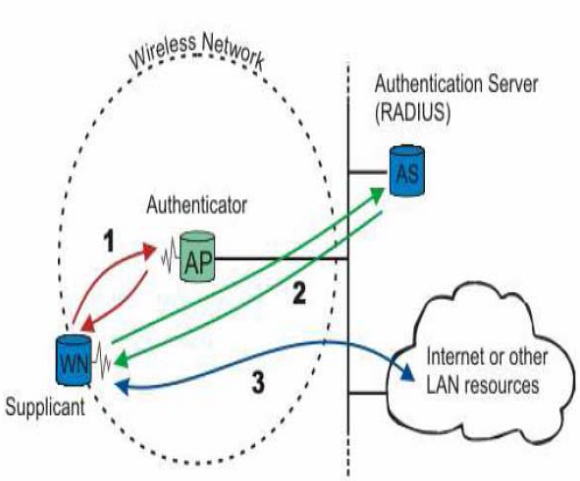
STANDAR KEAMANAN WIRELESS

Setelah mengetahui kelemahan, celah-celah keamanan, serta beberapa aktifitas penanganan keamanan pada jaringan Wireless maka selanjutnya akan ditinjau tentang standar keamanan wireless menurut IEEE(*Institute of Electrical and Electronics Engineers*). Model penanganan kemanan yang dilakukan seperti diatas semestinya mengacu pada standar yang dikeluarkan IEEE yang dinamakan standar IEEE 802.1x yang merupakan standar keamanan jaringan yang mempunyai banyak mekanisme untuk autentifikasi.

IEEE 802.1x atau sering disebut juga "*port based authentication*" merupakan standar yang pada awal rancangannya digunakan pada koneksi *dialup*. Tetapi pada akhirnya, standar 802.1x digunakan pula pada jaringan IEEE 802 standar. Teknik pengaman 802.1x ini akan mengharuskan semua pengguna jaringan wireless untuk melakukan proses otentikasi terlebih dahulu sebelum dapat bergabung dalam jaringan. Sistem otentikasinya dapat dilakukan dengan banyak cara, namun sistem otentikasi menggunakan pertukaran key secara dinamik. Sistem pertukaran key secara dinamik ini dapat dibuat dengan menggunakan *Extensible Authentication Protocol* (EAP). Sistem EAP ini sudah cukup banyak terdapat di dalam implementasi fasilitas-fasilitas di RADIUS.

Dalam metode ini, software key management dimasukkan pada perangkat WLAN client. Dalam asosiasi pertama dengan perangkat *Access Point (*AP), software tersebut akan memberitahukan pengguna untuk memasukkan identitas jaringan WLAN yang ingin dimasukki seperti username password misalnya. Identitas ini kemudian diteruskan ke EAP atau RADIUS server melalui AP untuk proses otentikasi. Ketika authentikasi berhasil, seperangkat encription key diberikan untuk perangkat AP dan juga client untuk dapat saling berkomunikasi. Namun, key ini hanya berlaku dalam satu sesi komunikasi saja. Ketika penggunanya melakukan roaming atau berpindah-pindah AP, maka encryption key yang dinamik ini akan dikirimkan oleh AP yang memilikinya ke seluruh AP yang terkoneksi dengannya.

Berikut merupakan skema dasar dari standar 802.1x.



Gambar 8. Skema Keamanan 802.1x

Keterangan :

1. Jika terdapat WN (*Wireless Node*) baru yang ingin mengakses suatu LAN, maka *access point* (AP) akan meminta identitas WN. Tidak diperbolehkan trafik apapun kecuali trafik EAP (*Extensible Authentication Protocol)*. WN yang ingin mengakses LAN disebut dengan *supplicant*. AP pada skema 802.1x merupakan suatu *authenticator*.
2. Setelah identitas dari WN dikirimkan, proses *authentifikasi supplicant* pun dimulai. Protokol yang digunakan antara *supplicant* dan *authenticator* adalah EAP, atau lebih tepatnya adalah *EAP encapsulation over LAN* (EAPOL) dan *EAP encapsulation over Wireless* (EAPOW).
3. Setelah proses authentifikasi selesai, *supplicant* dapat mengakses LAN secara biasa.

Sebelum authentifkasi berhasil, hanya port dengan jenis *uncontrolled* yang dibuka. Trafik yang diperbolehkan hanyalah EAPOL atau EAPOW. Setelah *supplicant* melakukan autentifikasi dan berhasil, port jenis *controlled* dibuka sehingga *supplicant* dapat mengakses LAN secara biasa. IEEE 802.1x mempunyai peranan penting dari standar 802.11i.

1. 802.11i

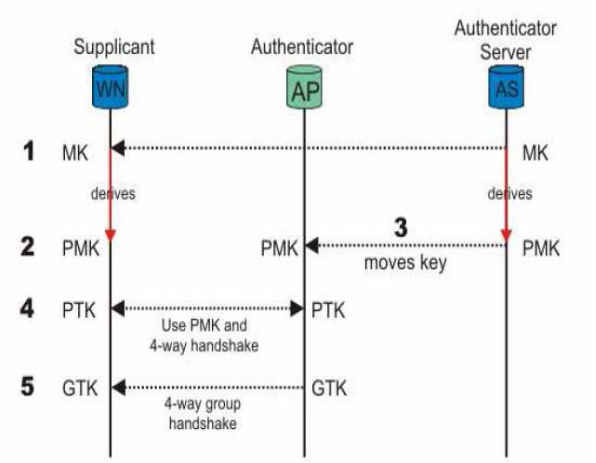
a. **WEP.** *Wired Equivalent Privacy* (WEP), merupakan bagian dari 802.11 standar. Sayang sekali WEP dirancang untuk dengan mudah dicrack. Tidak ada mekanisme authentifikasi, dan hanya menggunakan shared *key* (anda harus memasukkan key untuk bisa berkomunikasi). WEP menggunakan RC4 untuk teknik enkripsinya. Karena banyak sekali kelemahan pada WEP, maka IEEE menetapkan standar baru 802.11i. 802.1x mempunyai peranan penting dalam standar yang baru ini. WEP menggunakan sistem enkripsi untuk memproteksi pengguna WLAN dalam level yang paling dasar.

b. **802.11i.** Standar baru 802.11i, disahkan pada bulan Juni 2004, memperbaiki semua kelemahan WEP. Standar tersebut dibagi menjadi tiga ketegori, yaitu :

- *Temporary Key Integrity Protocol* (TKIP), merupakan solusi singkat untuk mengatasi kelemahan WEP. TKIP bisa digunakan pada peralatan 802.11 yang lama (dengan mengupdate *driver/firmware*-nya).
- *Counter Mode with CBC-MAC Protocol* (CCMP) [RFC2610] adalah protokol baru dan didesain dari dasar. Protokol tersebut menggunakan AES untuk algoritma enkripsinya. Karena algoritma ini membutuhkan lebih banyak *cpu resource*, maka peralatan 802.11 yang baru pun diperlukan. Tetapi CCMP juga bisa diemulasi dan diimplementasikan dengan software.
- 802.1x "*Port-Based Network Access Control*", dengan menggunakan TKIP atau CCMP, digunakan untuk authentifikasi.

802.11i mempunyai extended *key* manajemen, dideskripsikan sebagai berikut.

c. ***Key* Manajemen.** Untuk membuat *security policy* menggunakan algoritma enkripsi, maka key harus didistribusikan. Standar 802.11i mengimplementasikan cara manajemen *derivative key*. Untuk lebih jelasnya dapat dilihat pada gambar berikut.



Gambar 9. Manajemen dan distribusi key pada 802.11i

Keterangan :
Gambar diatas tersebut merupakan mekanisme manajemen dan distribus key pada 802.11i. Penjelasan dari no 1-5 adalah sebagai berikut :

1. Ketika *supplicant/Wireless Node* (WN) dan *Authentication Server* (AS) enyelesaikan proses authentifikasi, maka paket terakhir yang dikirimkan AS ke WN adalah *Master Key* (MK). Setelah MK dikirimkan, maka hanya WN dan AS yang tahu sehingga diperlukan mekanisme selanjutnya.
2. Keduanya (WN dan AS) menurunkan *key*, yang disebut dengan *Pairwise Master Key* (PMK), dari *Master Key*.
3. PMK dipindahkan dari AS ke *Authenticator* (AP). Hanya WN dan AS yang bisa menurunkan MK ke PMK, dan dengan PMK AP dapat mewakilkan AS untuk keputusan kontrol akses dari suatu WN. PMK merupakan suatu *symetric key* yang membatasi antara WN dan AP.
4. PMK dan *4-way handshake* digunakan antara WN dan AP untuk

menurunkan, menyetujui, dan memverifikasi *Pairwise Transient Key* (PTK). PTK merupakan koleksi dari beberapa operasional key yaitu:

a. *Key Confirmation Key* (KCK). Seperti namanya, key ini digunakan untuk konfirmasi PMK antara WN dan AP.

b. *Key Encryption key* (KEK), digunakan untuk mendistribusikan *Group Transient Key* (GTK).

c. *Temporal Key 1 & 2* (TK1/TK2), digunakan untuk enkripsi data.

5. KEK dan *4-way handshake* digunakan untuk mengirimkan *Group Transient Key* (GTK) dari AP ke WN. GTK adalah *shared key* diantara *supplicant* yang terhubung ke *authenticator* yang sama dan digunakan untuk men-*secure*kan *multicast*/*broadcast* trafik.

d. **WPA dan WPA2 (***WI-FI Protected Access*)**.** WPA dan WPA2 merupakan standar yang mempunyai mekanisme authentifikasi yang sama tetapi berbeda untuk teknik enkripsi yang digunakan. Pada WPA, teknik enkripsi yang digunakan adalah RC4 dengan TKIP sedangkan pada WPA2 digunakan teknik enkripsi AES dengan CCMP. Jadi dapat disimpulkan sebagai berikut:

- TKIP + 802.1x = WPA(1)
- CCMP + 802.1x = WPA2

Teknik ini merupakan teknik pengaman jaringan wireless LAN yang diklaim lebih canggih dari WEP. Dengan disertai teknik enkripsi yang lebih advanced dan tambahan pengaman berupa otentikasi dari penggunanya, maka WPA akan jauh lebih hebat mengamankan Anda pengguna WLAN.

2. EAP

Extensible Authentication Protocol (EAP) [RFC3748] merupakan universal authentifikasi framework yang banyak digunakan pada jaringan wireless dan koneksi *point-to-point*. Meskipun EAP tidak hanya terbatas digunakan pada jaringan wireless LAN dan bisa juga digunakan pada jaringan kabel LAN, tetapi EAP banyak diimplementasikan pada jaringan wireless LAN. EAP merupakan authentifikasi framework dan bukan terbatas pada satu mekanisme authentifikasi.

- **EAP-TLS**. EAP-TLS [RFC2716], adalah IETF standar dan banyak disupport oleh vendor peralatan wireless. EAP-TLS menawarkan tingkat keamanan yang tinggi, semenjak TLS dianggap sebagai teknik enkripsi yang sukses pada mekanisme SSL. TLS menggunakan *Public Key Infrastructure* (PKI) untuk mengamankan komunikasi antara *supplicant* dan *authentication server*. EAP-TLS adalah standar EAP wireless LAN. Meskipun EAP-TLS jarang digunakan, tetapi mekanismenya merupakan salah satu standar EAP yang paling aman dan secara universal disupport oleh semua manufaktur dari wireless LAN hardware dan software termasuk Microsoft.
- **EAP-MD5.** EAP-MD5 [RFC3748], merupakan IETF open standar tetapi menawarkan ting-kat keamanan yang rendah. Fungsi hash MD5 mudah diserang dengan metode *dictinary attack*, tidak ada mutual authentifikasi, dan penurunan kunci; sehingga membuatnya tidak cocok untuk dipakai dengan dinamik WEP atau WPA/WPA2 enterprise.
- **EAP-TTLS.** EAP-*Tunneled TLS* atau EAP-TTLS merupakan standar yang dikembangkan oleh *Funk Software* dan *Certicom*. Standar ini secara luas disupport dan menawarkan tingkat keamanan yang bagus. Standar ini menggunakan PKI sertifikat hanya pada *authentication server*.

- **PEAP**. *Protected EAP* (PEAP), sama seperti EAP-TTLS, memakai TLS-tunel. Sertifikat supplicant untuk PEAP tidak diperlukan, tetapi untuk sertifikat server (AS) dibutuhkan. PEAP dikembangkan oleh Microsoft, Cisco System, dan RSA Security.
- **EAP-MSCHAPv2.** EAP-MSCHAPv2 membutuhkan *username* dan *password* untuk melakukan mekanisme authentifikasinya. Secara dasar EAP-MSCHAPv2 merupakan en-kapsulasi EAP dari MSCHAPv2 dan biasanya digunakan pada PEAP-tunel. EAPMSCHAPv2 dikembangkan oleh Microsoft dan merupakan IETF draft.

3. RADIUS

Remote Authentication Dial-In User Service (RADIUS) memungkinkan beberapa alat *remote* akses untuk berbagi database otentikasi yang sama. Dia menyediakan sebuah titik pusat manajemen untuk semua akses network remote. RADIUS pada awalnya digunakan oleh ISP untuk authentifikasi dengan username/password sebelum dapat berkoneksi dengan jaringan ISP, dan biasanya adalah untuk user dial-up. RADIUS digunakan untuk *back-end authentication server* pada 802.1x. Selain RADIUS ada beberapa protokol AAA (*Authentication, Authorization, Accounting*) yang bisa juga digunakan yaitu TACACS, TACACS+, dan DIAMETER. RADIUS telah digunakan terutama untuk akses modem dari lokasi remote ke sebuah jaringan. Dukungan vendor seperti 3COM, CISCO dan Ascend terhadap RADIUS karena telah melakukan sebuah metode otentikasi terhadap user-user remote yang mencoba mengakses jaringan local melalui sebuah *firewall*. Meskipun dapat melakukan otentikasi yang kuat, namun RADIUS memiliki kelemahan yaitu spesifikasinya tidak mencakup enkripsi, dia juga tidak punya cara untuk memastikan integritas dari data setelah session dibuat.

KESIMPULAN

Teknologi wireless memiliki beberapa macam aplikasi teknologi yang memiliki karakteristik yang berbeda begitu juga dengan kelebihan dan kekurangan pada masing-masing teknologi tersebut. Namun begitu telah terdapat standar keamanan yang dapat diterapkan dalam pemakaian teknologi wireless. Untuk itu dalam penggunaannya setidaknya para user dan operator harus memenuhi standar keamanan yang ada agar keamanan pada perangkat teknologi yang digunakan juga aman.

DAFTAR PUSTAKA

1. Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley, 2005, "*Network Security Bible*", Wiley Publishing Inc.
2. Fuad, Reza, "Standar IEEE 802.1x : Teori dan Implementasi, internet, diakses 2007
3. http://budi.insan.co.id
4. http://id.wikipedia.net
5. http://www.drizzle.com/aboba/IEEE/rc4_ksaproc.pdf
6. http://www.intel.com
7. http://www.ristinet.com/
8. http://www.wikipedia.org
9. http://www.wimaxforum.org