STUDI PERANGKAT WIRELESS LAN DAN PENGAMAN DATA DI UNIVERSITAS MEDAN AREA

TUGAS AKHIR

Diajukan Untuk Memenuhi Persyaratan
Ujian Sarjana

Oleh :

ROYHOT HARIANJA
NIM : 06.812.0014

PROGRAM STUDI TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS MEDAN AREA
MEDAN
2010

STUDI PERANGKAT WIRELESS LAN DAN PENGAMAN DATA DI UNIVERSITAS MEDAN AREA

TUGAS AKHIR

Oleh :

ROYHOT HARIANJA

NIM : 06.812.0014

Disetujui :

Pembimbing I,	Pembimbing II,
(Ir.H.Usman Harahap)	**(Suprianto, ST.MT)**

Mengetahui :

Dekan	Ka. Program Studi,
(Ir. Hj. Hasniza, MT)	**(Ir. Yance Syarif)**

Tanggal Lulus :

RINGKASAN

Inovasi dibidang komunikasi data berkembang yaitu mencari layanan yang *fleksibel* dan *efisien* disegala aspek, serba mudah dan memuaskan. Untuk itu, dibutuhkanlah suatu jaringan yang mampu menghubungkan setiap *node* antar terminal yang akan saling berkomunikasi secara efisien. Teknologi ini dikenal dengan teknologi *Wireless LAN*. Seiring dengan perkembangan tersebut ditemukan berbagai masalah sering terputusnya, lambatnya koneksi antara jaringan dengan klien dan adanya pencurian data.

Teknologi wireless memanfaatkan radio frekuensi untuk melakukan interaksi atau komunikasi antara unit komputer. Dimana perangkat yang dibutuhkan seperti *access point, Wireless LAN Interface,* Antena dan beberapa perangkat lain. Masalah keandalan jaringan dan keamanan data merupakan salah satu aspek penting dari sebuah sistem informasi.

Menghindari jika sewaktu-waktu keamanan data tersebut dapat dipecahkan oleh orang lain maka harus dikontrol dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus yang disebut dengan *enkripsi*. Dan mengolah informasi tersebut menjadi informasi yang jelas dan tepat dengan tujuan agar dapat dapat dimengerti yang disebut dengan *deskripsi*.

Salah satu pengganggu kinerja jaringan *wireless* adalah jamming, dimana ditemukan banyaknya frekuensi saingan yang mengganggu kinerja Wireless LAN yang berasal dari handphone, modem, notebook, dan PDA. Dan untuk melindungi keamanan data adalah dengan proses *Autentikasi* yaitu proses yang terdiri dari SSID, MAC, *Autentikasi*, dan *Associated* yang bertujuan mengamankan data-data yang berupa *username*, *password*, pencurian data dan perusakan jaringan.

ABSTRACT

Innovation in the field of developing data communications is looking for a flexible and efficient service in all aspects, easy and satisfying. So, we needed a network capable of connecting each node between the terminal that would efficiently communicate with each other. This technology known as Wireless LAN technology. Along with these developments found in a variety of issues often cut off, slow network connection between the client and the theft of data.

Wireless technology utilizing radio frequency to make interaction or communication between the computer unit. Where the device is needed such as access point, Wireless LAN Interface, antenna and other some devices. The problem of network reliability and data security is one important aspect of an information system.

Avoid if at any time the data security can be solved by others, it must be controlled with making such information can not be read without the aid of specialized knowledge which is called encryption. And process that information into clear appropriate and information with the aim that can be understood that referred to the description.

One of the intruders is jamming wireless network performance, which found the number of frequencies that interfere with the performance of competing wireless LAN that originated from mobile phones, modems, notebooks, and PDAs. And to protect the security of data is to process authentication is a process that consists of the SSID, MAC, authentication, and the Associated aimed at securing data in the form of usernames, passwords, data theft and destruction of network.

DAFTAR ISI

RINGKASAN i

KATA PENGANTAR iii

DAFTAR ISI v

DAFTAR GAMBAR viii

DAFTAR TABEL ix

BAB I PENDAHULUAN

I.1. Latar Belakang 1

I.2. Perumusan Masalah 2

I.3. Tujuan Penelitian 2

I.4. Manfaat Penelitian 3

I.5. Batasan Masalah 3

I.6. Metoda Penelitian 4

I.7. Sistematika Penelitian 4

BAB II MENGENAL WIRELESS LAN

II.1. Pengertian Wireless LAN 5

II.2. Sejarah Wireless LAN 6

II.3. Spread Spectrum Technology 8

II.3.1. Direct Sequence Spread Spectrum (DSSS) 8

II.3.2. Frequency Hopping Spread Spectrum (FHSS) 10

II.4. Perbandingan DSSS dengan FHSS 12

II.5. Frequency Wireless LAN 13

II.6. Konfigurasi Jaringan Wireless LAN 14

BAB III METODOLOGI PENELITIAN

III.1. Standar Wireless LAN 17
III.1.1. Standar 802.11 18
III.1.2. Standar 802.11.b 18
III.1.3. Standar 802.11.a 19
III.1.4. Standar 802.11.g 20
III.1.5. Perbandingan Standar Wireless LAN 802.11.a/b/g 21
III.1.6. Kelebihan Dan Kekurangan Standar Wireless LAN 802.11.a/b/g 22
III.2. Keuntungan Wireless LAN 22
III.2.1. Mobilitas Tinggi 22
III.2.2. Kemudahan Dan Kecepatan Instalasi 23
III.2.3. Fleksibel 24
III.2.4. Menurunkan Biaya Kepemilikan 24
III.2.5. Scalable 24
III.2.6. Produktifitas 25
III.3. Perbandingan Wireless LAN dengan Jaringan Kabel 25
III.4. Kelemahan Wireless LAN 26
III.5. Jenis Serangan Pada Wireless LAN 27
III.5.1. Serangan Pasive (Passive Attacks) 27
III.5.2. Serangan Aktif (Active Attacks) 29
III.5.3. Jamming 31
III.5.4. Man In The Midle Attakcs 33

BAB IV PERANGKAT DAN PENGAMAN DATA

WIRELESS LAN

IV.1. Perangkat Utama 35

IV.1.1 Access Point 35

IV.1.2. Wireless Adapter (Wireless LAN) 39

IV.1.3. Antena 41

IV.1.3.1. Aksesori antena *Wireless LAN* 44

IV.2. Perangkat Bantu 47

IV.2.1. Switch 47

IV.2.2. Repeater 47

IV.2.3. Brigde 48

IV.2.4. Modem 49

IV.2.5. Kabel UTP 49

IV.2.6. Konektor 50

IV.3. Pengaman Data Wireless LAN 50

IV.3.1. SSID (Service Set Identifier) 51

IV.3.2. MAC Filtering 51

IV.3.3. Autentikasi 52

IV.3.4. Associated 53

BAB V KESIMPULAN DAN SARAN

V.1. Kesimpulan 54

V.2. Saran 55

DAFTAR PUSTAKA 56

LAMPIRAN 57

BAB I
PENDAHULUAN

I.1. Latar Belakang Masalah

Seiring dengan perkembangan teknologi di bidang komputer yang berkembang pada masyarakat modren, yang memiliki tingkat kebutuhan yang tinggi di bidang komunikasi terhadap layanan yang fleksibel serba mudah, serta memiliki efesiensi yang luas di berbagai aspek, maka salah satu teknologi yang mampu menyediakan kebutuhan tersebut adalah teknologi *Wireless LAN*.

Teknologi ini memerlukan proses pengiriman data dengan menggunakan frekuensi radio sebagai media transmisinya. Dengan hadirnya perangkat *Wireless LAN* diharapkan dapat mempermudah komunikasi internet, baik secara tulisan maupun suara bahkan sampai gambar bergerak.

Seiring dengan perkembangan *Wireless LAN* tersebut ditemukan adanya berbagai masalah yang sering terjadi. Masalah tersebut adalah sering putusnya koneksi antara jaringan dengan klien, sangat lambatnya koneksi *Wireless LAN* pada saat klien banyak yang terhubung ke jaringan dan adanya pencurian data berupa *username* dan *password* yang tidak di ketahui oleh klien sendiri.

Dengan adanya masalah-masalah tersebut seringkali klien merasa dirugikan karena harus kehilangan waktu mereka untuk menunggu koneksi Wireless LAN yang bagus dan sepi dari pengguna. Selain itu bagi klien yang kehilangan data berupa username dan *password* harus melapor kembali ke pusat komputer.

Maka untuk mengantisipasi hal tersebut perlu studi terhadap perangkat *Wireless LAN* dan pengamanan data untuk kenyamanan para pengguna *Wireless LAN.*

I.2. Perumusan Masalah

Fasilitas *Wireless LAN* dalam sebuah universitas sudah merupakan suatu keharusan yang harus diperoleh oleh setiap mahasiswa yang menjalani perkuliahan di universitas tersebut. Dengan tujuan agar setiap pengguna *Wireless LAN* tersebut dapat meningkatkan produktivitasnya.

Wireless LAN sendiri merupakan teknologi komunikasi yang berkembang yang memiliki kelemahan-kelemahan baik dalam keandalan jaringan dan pengamanan datanya. Oleh karena adanya gangguan yang terjadi pada jaringan *Wireless LAN* yaitu sering terputusnya atau lambatnya koneksi jaringan dengan klien maka sangat diperlukan peninjauan kembali perangkat-perangkat dan pengamanan data *Wireless LAN.*

Dan yang menjadi masalahnya adalah bagaimana cara mengamankan data dan membuat jaringan *Wireless LAN* yang lebih handal supaya klien merasa tidak diruguikan.

I.3. Tujuan Penelitian

Penelitian tugas akhir ini bertujuan untuk :

1. Mengetahui jenis-jenis perangkat *Wireless LAN* yang digunakan di Universitas Medan Area

2. Mencari penyebap sering lambatnya, atau terputusnya koneksi *Wireless LAN* di Universitas Medan Area
3. Mengetahui cara pengamanan data pengguna di Universitas Medan Area.
4. Mengetahui cara kerja *Wireless LAN*

I.4. Manfaat Penelitian

Manfaat yang diharapkan dalam penulisan penelitian ini adalah:

1. Bagi Peneliti

   Merupakan sarana untuk menerapkan ilmu pengetahuan yang diperoleh di bangku kuliah.

2. Bagi Akademis

   Penelitian ini diharapkan dapat menjadi accuan untuk dijadikan tolak ukur dan keberhasilan selama ini dalam mendidik dan membekali ilmu sebelum peneliti melakukan penelitiannya.

3. Bagi Universitas Medan Area

   Sebagai masukan untuk mengambil tindakan apabila terjadi gangguan pada perangkat wireless dan pada pengamanan data.

I.5. Batasan Masalah

Karena keterbatasan kemampuan peneliti, maka peneliti membuat batasan-batasan antara lain :

1. Membahas jenis-jenis perangkat *Wireless LAN* dan cara pengamanan *Wireless LAN*

2. Dalam hal ini pengamanan data menggunakan standar keamanan *Autentikasi*, yaitu suatu proses pengamanan data dengan menggunakan *username* dan *pasword* yang diperoleh dengan cara mendaftar di pusat komputer.
3. Mengetahui dan menganalisa cara kerja *Wireless LAN* di Universitas Medan Area

I.6. Metoda Penelitian

Metoda penelitian yang digunakan adalah dengan memperoleh data-data dari lapangan dan dengan menelaah buku-buku yang berkaitan dengan topik yang di bahas di atas.

I.7. Sistematika Penelitian

Adapun sistematika penulisan penelitian tugas akhir ini adalah Bab I Pendahuluan Berisi latar belakang masalah, tujuan penelitian , batasan masalah, metoda penelitian dan sistematika penelitian. Bab II : Mengenal *Wireless LAN* berisi tentang teori-teori yang berkaitan dengan *Wireless LAN*. Bab III : Metodologi Penelitian Pada bab ini diuraikan tentang standar, keuntungan, kelemahan, dan jenis-jenis serangan pada *Wireless LAN*.

Bab IV : Perangkat dan pengamanan *Wireless LAN* Berisi tentang perangkat *Wireless LAN* dan pengamanan *Wireless LAN* dan data-data yang di perlukan dalam penulisan Tugas Akhir ini. Bab V : Kesimpulan dan Saran Berisi tentang kesimpulan dan saran yang di dapatkan penulis dari penyusunan Tugas Akhir ini.

BAB II
MENGENAL WIRELESS LAN

II.1. Pengertian Wireless LAN

Istilah jaringan Nirkabel atau *Wireless LAN* adalah teknologi jaringan yang tidak menggunakan perangkat kabel yang umumnya dijumpai di dalam sebuah jaringan komputer dewasa ini. Teknologi ini sesuai dengan namanya *Wireless* yang artinya tanpa kabel, yaitu dengan memanfaatkan gelombang radio untuk melakukan interaksi atau komunikasi antar unit komputer. *Wireless LAN* pada dasarnya adalah sebuah perangkat radio komunikasi data yang mampu menghubungkan antar komputer atau sebuah komputer ke sebuah *Local Area Network (LAN)* ataupun sebaliknya.

Tentunya *Wireless LAN* dapat digunakan juga menghubungkan antar *LAN*, sehingga memungkinkan adanya *resource sharing* (penggunaan bersama) pada setiap komputer yang terhubung. Dengan menggunakan perangkat ini maka kita dapat membuat LAN tanpa menggunakan kabel data jenis *Unshield Twistted Pair (UTP)* yang umum di gunakan dalam jaringan komputer, di samping jenis-jenis kabel yang lainnya.

Dengan jaringan *Wireless LAN* ini memungkinkan para pengguna komputer terhubung tanpa kabel (*wirelessly*) ke dalam suatu jaringan. Sebuah *laptop* atau *PDA (Personal Digital Assistant)* yang dilengkapi dengan *PCMCIA (Personal Computer Memory Card Industry Association)* dapat digunakan secara mobile tanpa perlu mencolokkan *(plug in)* kabel apapun.

II.2. Sejarah Wireless LAN

Pada akhir 1970-an IBM mengeluarkan hasil percobaan mereka dalam merancang WLAN dengan teknologi *IR (Infa Red)*, perusahaan lain seperti *Hewlett-Packard (HP)* menguji WLAN dengan *RF (Radio Frequency)*. Kedua perusahaan tersebut hanya mencapai data rate 100 Kbps. Karena tidak memenuhi standar IEEE 802 untuk LAN yaitu 1 Mbps maka produknya tidak dipasarkan. Baru pada tahun 1985, *Federal Communication Commision (FCC)* menetapkan pita *Industrial, Scientific and Medical (ISM band)* yaitu 902-928 MHz, 2400-2483.5 MHz dan 5725-5850 MHz, sehingga pengembangan WLAN secara komersial memasuki tahapan serius.

Barulah pada tahun 1990 WLAN dapat dipasarkan dengan produk yang menggunakan teknik *spread spectrum* pada pita ISM, frekuensi terlisensi 18-19 GHz dan teknologi IR dengan data rate >1 Mbps. Pada tahun 1997, sebuah lembaga independen bernama IEEE membuat spesifikasi/standar WLAN pertama yang diberi kode 802.11. Peralatan yang sesuai standar 802.11 dapat bekerja pada frekuensi 2,4GHz, dan kecepatan *transfer* data maksimal 2 Mbps. Pada bulan Juli 1999, IEEE kembali mengeluarkan spesifikasi baru bernama 802.11b. Kecepatan transfer data teoritis maksimal yang dapat dicapai adalah 11 Mbps.

Pada saat hampir bersamaan, IEEE membuat spesifikasi 802.11a yang menggunakan teknik berbeda. Frekuensi yang digunakan 5Ghz, dan mendukung kecepatan *transfer* data teoritis maksimal sampai 54 Mbps. Gelombang radio yang dipancarkan oleh peralatan 802.11a relatif sukar menembus dinding atau penghalang lainnya. Jarak jangkau gelombang radio relatif lebih pendek dibandingkan 802.11b. Secara teknis, 802.11b tidak cocok dengan 802.11a.

Pada tahun 2002, IEEE membuat spesifikasi baru yang dapat menggabungkan kelebihan 802.11b dan 802.11a. Spesifikasi yang diberi kode 802.11g ini bekerja pada frekuensi 2,4Ghz dengan kecepatan transfer data teoritis maksimal 54 Mbps. Peralatan 802.11g kompatibel dengan 802.11b, sehingga dapat saling dipertukarkan.

Tercatat beberapa forum resmi yang dipelopori oleh industri-industri untuk pengembangan teknologi WLAN adalah sebagai berikut :

1. Apple Computer mendirikan *Wireless Information Network Forum (WIN Forum)* yang bertujuan untuk memanfaatkan pita frekuensi *Personal Comunication* Service (PCS) *unlicensed* untuk aplikasi data dan suara. Disamping itu, forum ini juga berusaha untuk membangun aturan-aturan untuk akses yang adil.
2. *European Telecomunication Standart Institude (ETSI)* yang mempelopori pengembangan *High Peformance Radio Local Area Network (HIPERLAN)* yang menfokuskan diri pada pita frekuensi 5.12-5.30 GHz dan 17.1-17.3 GHz.
3. IEEE 802.11 yang dipelopori oleh *Institude Electrical and Electronics Engineer (IEEE)* dan berfokus pada pita ISM dengan memanfaatkan teknik *Spread Spectrum (SS),* yaitu *Direct Sequence (DS)* dan *Frequency Hopping (FH).* Pada kenyataannya, akhirnya standart inilah yang paling luas penggunaanya.

II.3. Spread Spectrum Techonlogy

Proses pengiriman data melalui frekuensi radio dilakukan dengan teknik *Spread Spectrum*, yakni sebuah teknologi modulasi yang di rancang agar data dapat lebih tahan terhadap interferensi. *Wireless LAN* mentransfer data melalui udara dengan memancarkan gelombang elektromagnetik dengan menggunakan teknologi *Spread Spectrum Technology (SST).* Pada implementasinya, teknologi *spread spectrum* melakukan pendekatan, yakni *Direct Sequence Spread Spectrum* dan *Frequency Hopping Spread Spectrum.*

II.3.1. Direct Sequence Spread Spectrum (DSSS)

Pada pendekatan *direct sequence spread spectrum*, sebuah *bit* dikonversi ke dalam beberapa *chip*. Sinyal ditransfer ke dalam pita frekuenci terterntu yang tetap sebesar 17 MHz. Prinsip dari metoda *direct sequence* adalah memancarkan sinyal dengan lebar pita 17 MHz dengan pemakaian pelapisan kode atau *signature* untuk mengurangi *interferensi* dan *noise*. Kekurangan metode demikian adalah data 1 *bit* diwakili oleh beberapa bit. Misalnya, 1 *bit* menggunakan *bandwidth* 1 MHz. Jika data 1 *bit* dibentuk oleh 11 *chip* dimana masing-masing *chip* membutuhkan bandwidth sebesar 22 MHz.

If the data bit was : 1001

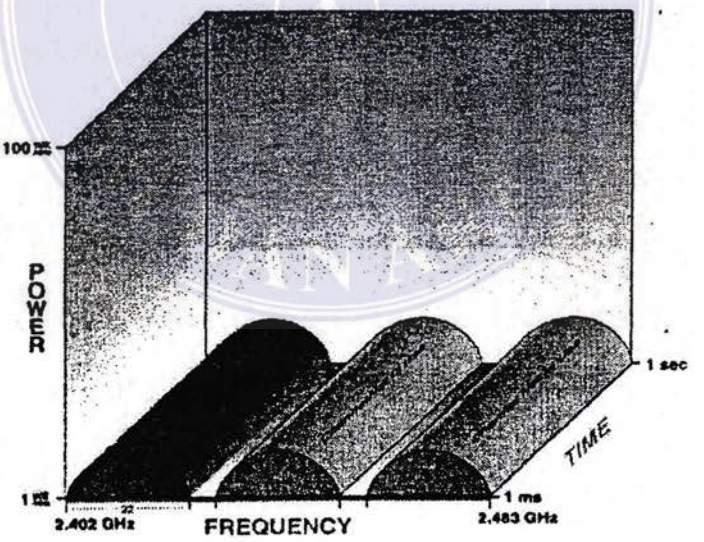
Chipping Code is : 1=00110011011 0=11001100100

Transmited data would be :

00110011011	11001100100	11001100100	00110011011
1	0	0	1

Pada saat sinyal dipancarkan, maka setiap paket data diberi kode berurut untuk sampai ke tujuan dan pada perangkat tujuan semua sinyal yang dipancarkan akan diterima dan diproses serta difilter sesuai dengan urutan kode yang masuk. Kode yang tidak sesuai akan diabaikan dan kode yang sesuai akan diproses lebih lanjut.

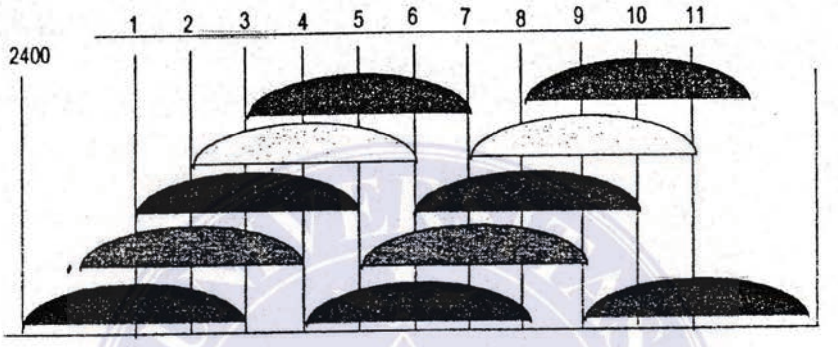
Teknik pembuatan kode seperti ini disebut dengan teknik *chipping*. Semakin panjang bit chip tersebut, maka semakin baik data yang dikirimkan tetapi juga akan memakan kapasitas *bandwidth* yang tersedia. Selain itu, dengan menggunakan metode DSSS akan dapat mengurangi serangan-serangan yang mungkin terjadi mengingat dayanya yang cukup rendah, sehingga dianggap sebagai *noise* jaringan oleh penyerang.



Gambar 2.1. Pola Direct Sequence Spread Spectrum
Sumber : Mengenal *Wireless LAN (WLAN)*, Zaenal Arifin, Penerbit Andi hal 4.

Dari gambar 2.1. terlihat bahwa DSSS menggunakan tiga macam *channel* yang tidak *overlapping*, sehingga tidak akan terjadi *interferensi* satu sama lain.

Dengan menggunakan metode ini, maka dapat diimplementasikan sebuah area dengan tiga macam *channel* yang tidak *overlapping*, sehingga tidak akan terjadi interferensi satu sama lain. Dengan menggunakan metode ini, maka dapat diimplementasikan sebuah area dengan tiga macam *Access Point (AP)*.



Gambar 2.2. Pembagian channel pada teknik DSSS
Sumber : Mengenal *Wireless LAN (WLAN)*, Zaenal Arifin, Penerbit Andi hal 5.

Dengan memanfaatkan lebar *bandwidth* yang tersedia, metode *Direct Sequence* dapat membentuk kurang lebih 11 *chanel* dan masing-masing *chanel* memiliki lebar 22 MHz. Dari chanel-chanel yang terbentuk, ada tiga channel yang tidak saling membentuk irisan *(overlap)*. Dengan demikian, dalam sebuah area kita dapat memasangkan tiga *access point* yang tidak saling mempengaruhi satu dengan yang lainnya.

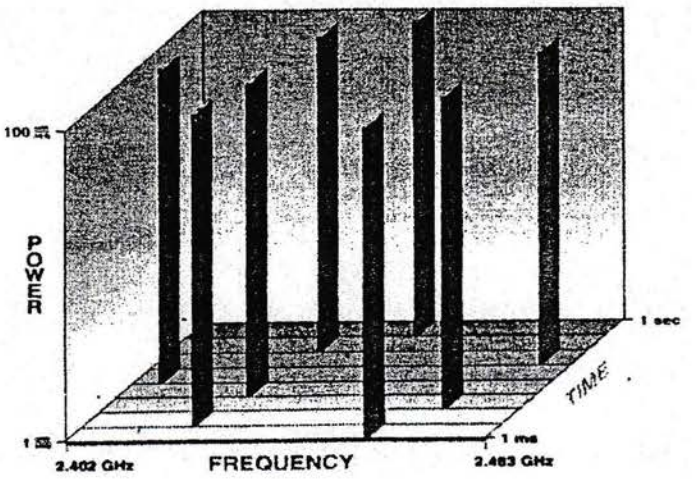
II.3.2. Frequency Hopping Spread Spectrum.

Metode *frequency hopping* memiliki 79 *channel* dan masing-masing *channel* diwakili oleh 1 MHz. Perubahan *frequency hopping* dilakukan tiap 0,4 detik. Jika terkena *interferensi* pada sebuah *frequency*, maka data akan dikirim ulang pada *frequency* berikutnya. Sinyal ditransfer secara bergantian dengan

menggunakan *frekuency* 1 MHz atau dalam rentang pita *frekuency* tertentu yang tetap. Prinsip dari metoda *Frequency Hopping* adalah menggunakan pita yang sempit yang bergantian untuk memancarkan sinyal radio. Secara periodik antara 20-400 ms (milidetik) sinyal berpindah dari kanal *frequency* lainnya. Metode ini harus diketahui oleh kedua belah pihak, yaitu penerima dan pengirim.

Pita *frequency* 2.4 GHz dibagi-bagi ke dalam beberapa sub bagian yang disebut *channell* / kanal. Salah satu standar pembagian kanal ini adalah sistem *ETSI (European Telecommunication Standart Institute)* dengan membagi kanal yang dimulai dengan kanal 1 pada *frequency* 2.412 MHz, kanal 2 2.417 MHz, kanal 3 2.422 MHz, dan seterusnya setiap 5 MHz bertambah sampai kanal 13.

Teknologi FHSS ditujukan untuk menghindari gangguan sinyal pada saat sinyal ditransfer , secara otomatis perangkat FHSS akan memilih *frequency* tertentu yang lebih baik baik untuk transfer data. Jika ada paket data yang hilang akan dilakukan retransimisi. Kondisi ini menjadikan satu keuntungan dibandingkan dengan DSSS. Teknologi DSSS dan FHSS tidak saling *interoporable*. Artinya perangkat DSSS tidak akan bisa melakukan koneksi ke perangkat FHSS maupaun sebaliknya.



Gambar 2.3. Pola Frequency Hopping Spread Spectrum
Sumber : Mengenal *Wireless LAN (WLAN),* Zaenal Arifin, Penerbit Andi hal 5.

II.4. Perbandingan DSSS dengan FHSS

Frequency hopping tidak menggunakan *processing gain* karena tidak menggunakan sistem penyebaran sinyal. *Processing gain* sebenarnya akan mengurangi kerapatan power dalam memproses transmisi. Karena FHSS tidak menggunakan *processing gain, frequency hopper* membutuhkan power yang lebih tinggi untuk melakukan transmisi dan menghasikan rasio *Signal to Notice Ratio (S/N)* yang sama.

Saat menggunakan *frequency hopping,* sinkronisasi pengirim dan penerima sinyal sangat sulit dilakukan, sehingga perlu untuk mengatur kedua peralatan ini dengan waktu dan *frequency* yang sama. Oleh karena itu, FHSS membutuhkan waktu yang lama dalam mencari sinyal, untuk kemudian menggunakannya.

Sementara itu, DSSS dapat dengan cepat melakukan *lock in* saat power dinyalakan, sehingga peralatan DSSS mempunyai waktu *latency* yang lebih

rendah pada keseluruhan transmisi. Secara keseluruhan, DSSS menggunakan *bandwidth* lebih tinggi bila dibanding dengan sistem FHSS.

II.5. Frequency Wireless LAN

Frequency yang digunakan oleh WLAN adalah menggunakan band *ISM (Industrial, Scientific, and Medical)* yang terdiri dari tiga band yaitu 900 MHz, 2,4 GHz, dan 5 Ghz. Secara rinci *frequency* yang digunakan beserta karakteristik *frequency* tersebut dapat dilihat pada tabel di bawah ini.

Tabel. 2.1. Pita Frequency ISM

Spesifikasi Frequency	**915 MHz**	**2,4 GHz**	**5,8 GHz**
Frequency	902-928MHz	2400-2483,5MHz	5725-5850 MHz
Bandwidth	25 MHz	83,5 MHz	125 MHz
Jangkauan Transmisi	Paling Jauh	Sedang	Pendek
Pemakaian	Sangat Ramai	Sepi	Sangat Sepi
Delay	Beasr	Sedang	Kecil
Sumber Interferensi	Banyak	Sedang	Sedikit

Sumber : Teknologi *Wireless LAN* dan Applikasinya, Gunadi, PT. Elex Media Komputindo hal 112.

Khusus pada pita *frequency* 2.4 GHz, alokasi spektrumnya berbeda antar negara di dunia.

Tabel 2.2. Spectrum WLAN pada pita frequency 2,4 GHz

Region	Alocated Spectrum
US	2.4000-2.4835 GHz
EUROPE	2.4000-2.4835 GHz
JAPAN	2.471-2.497 GHz
FRANCE	2.4465-2.4835 GHz
SPAIN	2.445-2.475 GHz

Sumber : Teknologi *Wireless LAN* dan Aplikasinya, Gunadi, PT. Elex Media Komputindo hal 112.

Namun demikian, biasanya *AP (Acces Point)* WLAN mampu menyediakan ke lima standar *frequency* di atas, tergantung administrator dalam melakukan pemilihan *frequency* yang akan digunakan.

II.6. Bentuk Konfigurasi Jaringan Wireless LAN

Bentuk konfigurasi jaringan *Wirelees LAN* terdiri dari :

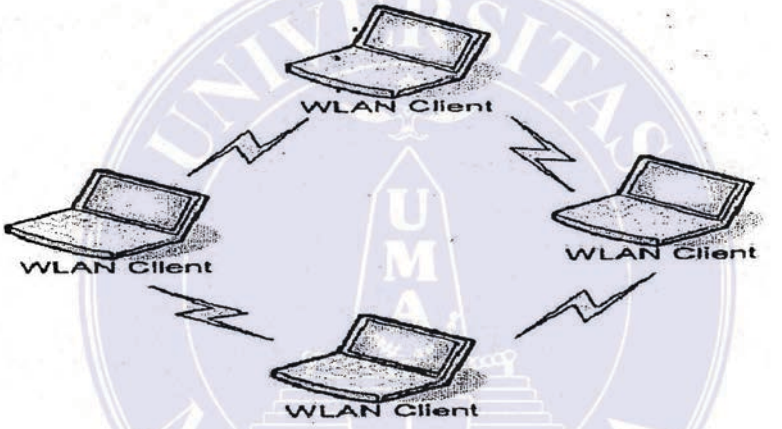
1. *Ad-Hoc (Peer to Peer)*

Standarisasi IEEE 802.11 mendefenisikan protokol dalam dua tipe jaringan, yaitu jaringan *Ad Hoc* dan *Klient/Server*.

Jaringan *Ad-Hoc* merupakan jaringan sederhana di mana komunikasi terjadi di antara dua perangkat atau lebih pada cakupan area tertentu tanpa harus memerlukan *access point* atau *server*. Standarisasi ini merupakan etiket untuk setiap perangkat jaringan dalam melakukan akses media wireless. Metode ini meliputi penentuan pemberian permintaan koneksi pada sebuah media untuk

memastikan *throughput* yang maksimal untuk pengguna dalam menerima layanan.

Komunikasi *Ad Hoc* menggunakan media gelombang radio satu dengan yang lain, dan peralatan ini mengenal peralatan RF lain dalam cakupan sinyal yang berdekatan, sehingga komunikasi dapat dilakukan. Jaringan *Ad Hoc* dapat digunakan pada *computer*, *notebook, laptop,* atau peralatan *handled* lain yang membutuhkan transfer data mobile dalam lingkup yang kecil, dan tentunya yang mempunyai peralatan RF yang sama dan telah mendukung jaringan *Ad Hoc*.



Gambar 2.4. Bentuk konfigurasi Ad-hoc
Sumber : Instalasi *Wireless LAN*, Winarno Sugeng, Penerbit Informatika hal 59.

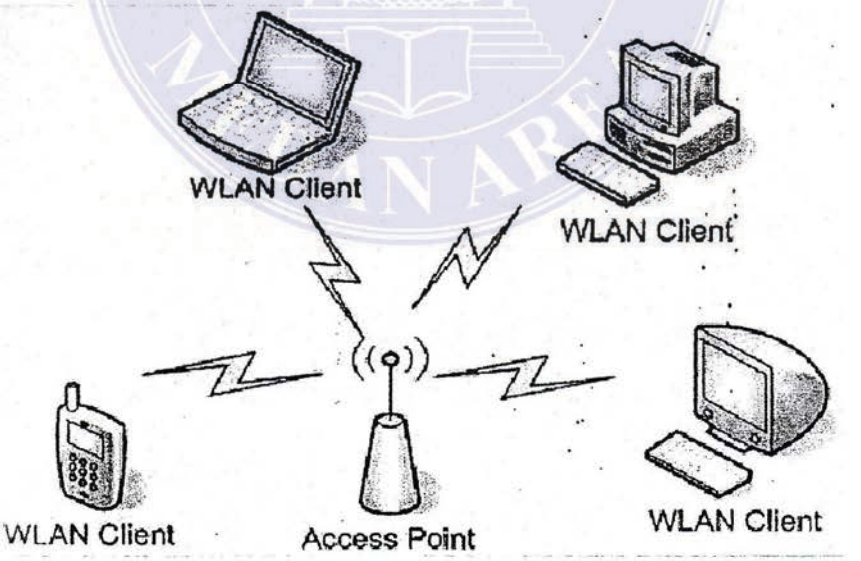
2. *Client/Server and Access Point*

Jarinngan *client/server* menggunakan *access point* sebagai pengatur alokasi waktu transmisi untuk semua perangkat jaringan dan mengijinkan perangkat mobile melakukan proses *roaming* dari sel-sel. *Access point* digunakan untuk menangani lalu lintas dari *radio mobile* ke perangkat yang menggunakan kabel maupun pada jaringan *wireless*.

Access point juga digunakan untuk melakukan pengaturan lalu lintas jaringan dari *mobile radio* ke jaringan kabel atau dari *backbone* jaringan *wireless*

klient/server. Pengaturan ini digunakan untuk melakukan koordinasi dari semua *node* jaringan dalam menggunakan layanan dasar jaringan serta memastikan penanganan lalu lintas data dapat berjalan dengan sempurna. *Access point* akan merutekan aliran data antara pusat jaringan dengan jaringan *wireless* yang lain. Dalam sebuah WLAN, pengaturan jaringan akan dilakukan oleh *access point* pusat yang mempunyai performa *throughput* yang lebih baik.

Jaringan yang menggunakan access point sering disebut *multipoint RF network*. Tipe jaringan *wireless* ini mempunyai beberapa station dengan *RF transmiter* dan *reciever*, dimana setiap stasiun akan berkomunikasi ke peralatan pusat *access point* ini atau sering disebut *wireless bridge*. Pada sistem RF, *wireless bridge* disebut *wireless access point (WAP)*. WAP menyediakan koneksi secara transparan ke *host* LAN melalui koneksi *ethernet* dan jaringan metode *wireless*.



Gambar 2.5. Bentuk Konfigurasi Insfrastruktur
Sumber : Instalasi *Wireless LAN*, Winarno Sugeng, Penerbit Informatika hal 60.

BAB III

METODOLOGI PENELITIAN

III.1. Standart Wireless LAN

Dewasa ini teknologi *WLAN (Wireless Local Area Network)* atau LAN tanpa kabel telah begitu akrab di kalangan dunia IT maupun yang bukan IT. Hal ini dibuktikan dengan semakin banyaknya pengguna WLAN baik untuk lingkunan kampus, perhotelan, perkantoran, perbankan, dan pusat-pusat perbelanjaan. Di samping telah berkembang hampir di semua segmen penggunanya, perkembangan WLAN baik dari sisi standar dan pertumbuhanya juga berkembang secara pesat.

Pertumbuhan pengguna WLAN di atas di dukung oleh beberapa alasan, seperti standar yang makin matang, kebutuhan akses *mobile* bagi pengguna, kemudahan mendapatkan perangkat, dukungan *vendor*, serta dukungan dari *vendor PC* dan *Laptop*. Khusus dukungan dari *vendor PC*, hal ini di buktikan dengan semakin banyaknya WLAN *card* yang dimasukkan kedalam *notebook (built in).*

Dalam bab ini akan dibahas secara detail terutama mengenai aspek standar WLAN khususnya 802.11a, 802.11b, 802.11g. Hal ini disebabkan standar tersebut merupakan standar yang paling banyak digunakan di pasaran dan akan terus berkembang dalam beberapa tahun kedepan. Faktor lainnya adalah, fleksibilitas dan ketiga standar tersebut mampu mendukung kecepatan transfer data.

III.1.1. Standar 802.11

Merupakan standar WLAN yang mampu menyediakan kecepatan data 1 atau 2 Mbps pada pita 2.4 GHz menggunakan *frequency hopping spread spectrum (FHSS)* atau *direct sequence spread spectrum (DSSS).*

III.1.2. Standar 802.11.b

Merupakan standar WLAN yang lebih dahulu ada dibanding 802.11a dan 802.11g dengan kecepatan 11 Mbps dan menggunakan frekuensi 2,4 GHz. Kecepatan standar ini tergantung dari beberapa faktor, seperti jarak, gangguan, hambatan dan kualitas sinyal yang sampai kepada penerima.

Standar 802.11b menggunakan dua metode pengkodean yang berbeda, yaitu FHSS dan DSSS. FHSS menyebarkan komunikasi melewati 75 MHz *subchannel* secara terus menerus sedangkan DSSS memecah pita frekuensi menjadi 14 *overlap* 22 MHz saluran dan menggunakannya satu demi satu.

Karakteristik standar 802.11b adalah sebagai berikut :

1. 802.11b-1999.
2. *Range 50-100 m* (tergantung dari hambatan).
3. *Indoor / Outdoor / Point to point (high gain external antennas).*
4. *Throughtput* maksimum 11 Mbit/s (5.5,2.1 Mbps)
5. Faktor penghambat, seperti logam, dingding, air.
6. Bekerja pada pita ISM 2,4 GHz.
7. 14 *overlapping channel* (berbeda *channel* berbeda negara).
8. Area jangkauan lebih luas yang dapat digunakan diruangan terbuka , semi terbuka, ataupun bersekat.
9. Memungkinkan *roaming* antar *zona* WLAN.

III.1.3. Standar 802.11.a

Merupakan perluasan dari standar 802.11 yang digunakan pada wireless LAN dan menyediakan kecepatan sampai dengan 54 Mbps pada pita frekuensi 5 GHz. 802.11a menggunakan *orthogonal frequency division multiplexing (OFDM)* yang mengencoding *scheme* lebih baik dibandingkan dengan FHSS dan DSSS. Cakupan 802.11a lebih kecil dibandingkan dengan 802.11b dan 802.11g.

Perbedaan mendasar 802.11a dengan 802.11g adalah bahwa 802.11a beroperasi pada pita frekuensi 5 GHz dengan 12 chanel *non-overlapping* yang terpisah. Dan sebagai hasilnnya, kita dapat mempunyai 12 *access point* yang disetting untuk channel yang berbeda pada area yang sama, tanpa adanya ganguan RF lebih kecil, karena frekuensi 5 GHz lebih sedikit digunakan oleh operator *wireless*.

Salah satu masalah besar yang terdapat pada 802.11a adalah tidak cocok dengan jaringan 802.11b atau 802.11g. Dengan kata lain, user yang menggunakan radio card 802.11b atau 802.11g tidak akan dapat terhubung secara langsung dengan akses point pada 802.11a.

Seperti halnya 802.11g, 802.11a juga mengirimkan data dengan kecepatan sampai 54 Mbps dengan kemungkinan perluasan data rate tinggi dengan mengkombinasikan *channel*. Berkaitan dengan frekuensi yang lebih tinggi, maka cakupan sekitar 80 kaki.

Karakteristik standar 802.11a adalah :

1. 2001 (802.11a-1999)
2. *Bandwidth* maksimum 54 Mbps (normalnya sekitar 20 Mbps)
3. Bekerja pada pita ISM 5 GHz

4. Lebih banyak *overlapping channel (12 chanel)*
5. *8 dedicated to indoor*
6. *4 to point to point*
7. Tidak kompatibel dengan standar sebelumnya (802.11b)
8. Pemanbahan jumlah *acess point* untuk memperbesar *coverage.*

III.1.4. Standar 802.11g

Standar 802.11g merupakan perluasan dari 802.11b. Basis mayoritas *Wireless LAN* saat ini adalah 802.11g yang akan memperluas data rate 802.11b sampai dengan 54 Mbps pada pita frekuensi 2,4 GHz yang menggunakan teknologi *orthogonal frequency division multiplexing (OFDM).*

Sama seperti 802.11b, 802.11g juga beroperasi pada pita frekuensi 2,4 GHz dan *bandwidth* sinyal menggunakan kira-kira 30 MHz. Dibandingkan dengan 802.11a, 802.11g yang menggunakan pita frekuensi 2,4 GHz mempunyai jangkauan yang lebih tinggi dibanding dengan produk 5 GHz untuk data *rate* yang sama.

Perlu di catat bahwa dalam kaitannya dengan gangguan di pita frekuensi 2.4 GHz jika dibanding dengan pita frekuensi 5 GHz, maka cakupan produk 802.11g akan sangat dipengaruhi oleh *noisy.* Implementasi spesifik dari *vendor* berbeda, seperti *power output*, kepekaan penerima, desain antena, dan faktor lain juga akan mempengaruhi cakupan tersebut.

Karakteristik standar 802.11g adalah sebagai berikut :.

1. Bekerja pada pita frekuensi 2.4 GHz.
2. *Throughput* maksimum 54 Mbps (Net 24.7 Mbps).

3. *A single wireless card / Acess point.*
4. Kompatibel dengan 802.11b.
5. Transfer data lebih besar dibanding 802.11b.
6. Dapat menjangkau area yang lebih luas.

III.1.5. Perbandingan Standart Wireless LAN 802.11.a/b/g

Tabel 3.1. Perbandingan Standar *Wireless LAN* 802.a/b/g

	802.11a	802.11b	802.11g
Frekuensi	5GHz	2,4 GHz	2,4GHz
Data Rate	54 Mbps	11 Mbps	54 Mbps
Modulasi	OFDM	CCk	OFDM
Avaliable bandwidth	300 MHz	83,5 MHz	83,5 MHz
Data rate per Channel	6,9,12,18,24,36,48, 54 Mbps	1,2,5,11 Mbps	1,2 ,6,9,11, ,18, 24, ,48,54 Mbps
Kompatibilitas	Tidak kompatibel b	Mature	Kompatibel b
Coverage	25-50 m	30-75 m	30-75 m
Jumlah non overlapping channel	8	3	3
Harga	Lebih mahal	Murah	Agak mahal

Sumber : Teknologi *Wireless LAN* dan Aplikasinya, Gunadi, PT. Elex Media Komputindo Hal 119.

III.1.6. Kelebihan Dan Kekurangan Standar Wireless LAN 802.11.a/b/g

Tabel 3.2. Kelebihan Dan Kekurangan Standar *Wireless LAN* 802.11.a/b/g

Standar	Kelebihan	Kekurangan
802.11a	Spekturm lebih besar dibanding 802.11b. Dapat digunakan dengan komplemen jaringan 802.11b. bandwidth yang lebih besar (54 Mb). Potensi interferensi lebih sedikit (5 GHz). Mempunyai lebih banyak non-overlapping chanel.	Area jangkauan sempit. Tidak kompatible dengan standar sebelumnya.
802.11b	Reliable. Jangkauan luas. Mudah di integrasikan dengan jaringan yang menggunakan kabel.	Kecepatan lebih rendah (11 Mbps) Frekuensi crowded
802.11g	Kompatibel dengan 802.11b. Transfer data lebih besar dibandingkan dengan 802.11b. jangkauan lebih besar dibanding 802.11a. Lebih cepat dibandingkan dengan 802.11b (24 Mb vs 11 Mb).	Frekuensi crowded.

Sumber : Teknologi *Wireless LAN* dan Aplikasinya, Gunadi, PT. Elex Media Komputindo Hal 120.

III.2. Keuntungan Wireless LAN

Ketergantungan bisnis, mahasiswa dan lainnya terhadap jaringan dan juga perkembangan yang sangat pesat dari internet, memberikan keuntungan terhadap perkembangan aplikasi dari *Wireless LAN*. Saat ini pemanfaatan *Wireless LAN* telah banyak digunakan baik untuk aplikasi internal perusahaan *(privat)* atau untuk lokasi publik (*hotspot).* Dengan semakin banyaknya pemakaian *Wireless LAN*, maka menunjukkan bahwa adanya keuntungan yang lebih banyak menggunakan *Wireless LAN* dibanding kerugiannya.

III.2.1. Mobilitas Tinggi

WLAN memungkinkan klien untuk mengakses informasi secara *real-time* sepanjang masih dalam jangkauan WLAN, sehingga meningkatkan kualitas layanan dan produktifitas yang tidak mungkin dapat diberikan oleh jaringan LAN biasa. Pengguna di manapun berada baik di area kantor bahkan di area publik

(hotspot) akan selalu dapat tersambung ke internet. Dengan demikian akan mendukung komunikasi suara, data, dan informasi yang lebih cepat.

Untuk penggunaan dalam area perkantoran, WLAN sangat mendukung untuk aplikasi bergerak *(mobile).* Sebagai contoh, seorang karyawan yang sering berpindah ruangan (diruang rapat, ruang kerja, kantin, maupun *lobby*) akan selalu terhubung ke jaringan internet, bila jangkauan WLAN telah memenuhi semua lokasi.

III.2.2. Kemudahan dan Kecepatan Instalasi

Instalasi WLAN sangat mudah dan cepat tanpa harus menarik dan memasang kabel melalui dinding atau atap. Kabel digunakan hanya untuk menghubungkan *access point (AP)* ke jaringan *(HUB/switch/router),* sedangkan koneksi dari stasiun komputer pelanggan komputer yang terhubung ke jaringan adalah melalui frekuensi radio *(wirelessly).* Lain halnya, bila menggunakan *wired LAN,* maka setiap *station* komputer yang tersambung ke jaringan LAN akan memerlukan kabel satu per satu ke *HUB/switch.*

Analoginya adalah jaringan telepon dengan media kabel tembaga yang terdapat di rumah-rumah, di mana tiap nomor telepon dihubungkan satu persatu ke sentral telepon. Dengan analogi ini, bisa di bayangkan kecepatan instalasi *Wiereless LAN* bila dibandingkan dengan wired LAN (LAN dengan menggunakan kabel UTP).

III.2.3. Fleksibel

Dengan teknologi WLAN sangat memungkinkan untuk membangun jaringan pada area yang tidak mungkin atau sulit untuk dijangkau oleh kabel. Misalnya, di kota-kota besar, di tempat-tempat yang tidak tersedia infrastruktur kabel, WLAN dapat digunakan untuk menggantikan teknologi *Leased-Line*.

Contoh penggunaan WLAN yang fleksibel sangat mudah dideteksi, bila ditujukan bagi bagian/departemen yang sering mengalami rotasi. Dengan WLAN apa pun perubahan lokasi kerja, maka perubahan posisi meja tidak akan berpengaruh. Lain halnya bila menggunakan *Wired* LAN, maka tentu sangat diperlukan perlukan perbaikan perkabelan.

III.2.4. Menurunkan Biaya Kepemilikan

Meskipun biaya infestasi awal untuk perangkat keras WLAN lebih mahal dibandingkan dengan LAN konvensional, namun biaya instalasi dan perawatan jaringan WLAN lebih murah, sehingga secara total dapat menurunkan biaya besar kepemilikan. Di samping itu, sangat cocok untuk lingkungan dinamis, dimana sering terjadi perpindahan, penambahan atau perubahan posisi kerja.

III.2.5. Scalable

WLAN dapat digunakan dengan berbagai topologi jaringan sesuai dengan kebutuhan instalasi atau spesifikasi. Mulai dari jaringan independen yang hanya terdiri atas beberapa klien saja, sampai jaringan infrastruktur yang terdiri atas ratusan klien.

Proses implementasi WLAN dapat dilakukan secara bertahap (*gradual*) sesuai dengan kebutuhan. Misalnya, untuk tahap awal hanya memasang 1 AP, kemudian berkembang menjadi beberapa AP sesuai dengan kebutuhan.

III.2.6. Produktivitas

Dengan dukungan teknologi WLAN, maka setiap orang akan dapat selalu terhubung ke internet dalam jangkauan tertentu. Dengan dukungan perangkat bergerak, maka setiap orang dapat cepat merespon kebutuhan nya. Bagi kalangan mahasiswa ini sangat menguntungkan karena dapat mengakses internet untuk mencari apa yang mereka butuhkan. Yang kemudian dapat menigkatkan produktivitas mahasiswa dalam mengerjakan tugas dan juga berkarya.

III.3. Perbandingan Wireless LAN Dengan Jaringan Kabel

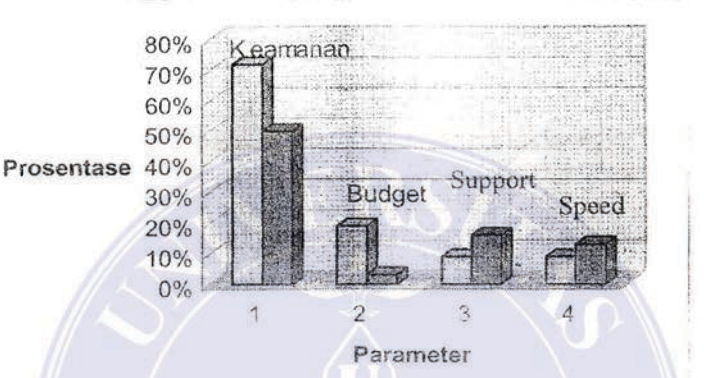
Tabel 3.3. Perbandingan Wireless LAN dengan jaringan kabel

Wireless LAN	Jaringan kabel
Pada WLAN dalam proses transmisi datanya menggunakan Radio Frekuensi (RF) dan tidak menggunakan kabel.	Pada jaringan kabel dalam proses pengiriman datanya harus menggunakan kabel sebagai media transmisi datanya
Dalam WLAN, klien dapat bergerak secara mobile atau berpindah-pindah tempat tanpa harus memcolokkan kabel terlebih dahulu untuk melakukan koneksi	Klien di tuntut untuk tidak berpindah-berpindah karena panjang kabel sangat dibatasi sesuai kebutuhan.
WLAN lebih fleksibel karena dapat menjangkau tempat-tempat yang tidak dapat dijangkau oleh kabel.	Tidak fleksibel karena klien harus mencari kabel jaringan untuk mencolokkan terlebih dahulu untuk dapat melakukan interaksi ke jaringan.
Dalam jaringan WLAN kabel hanya digunakan sebagai tulang punggung penghubung antara switch dan AP	

Sumber : Internet

III.4. Kelemahan Wireless LAN

Selain keuntungan-keuntungan di atas, WLAN juga memiliki beberapa kelemahan atau faktor penghambat. Dari beberapa hasil survey diperoleh, bahwa faktor keamanan merupakan faktor yang utama sebagai penghambat perkembangan WLAN.



Gambar 3.1. Faktor penghambat penggunaan WLAN
Sumber : Teknologi Wireless LAN dan Aplikasinya, Gunadi, PT. Elex Media Komputindo hal 8.

Dari gambar di atas, terlihat bahwa faktor autentikasi atau keamanan merupakan masalah utama dalam hal implementasi WLAN. Banyak sekali tipe serangan yang dapat terjadi pada sistem WLAN. Sebagai informasi bahwa sebenarnya WLAN sendiri mempunyai sistem keamanan, namun sangat terbatas.

Kelemahan WLAN lainnya, yaitu pada tingkat kecepatannya. Pada umumnya WLAN saat ini dapat menyediakan *data rate* hingga 54 Mbps dan 11 Mbps, namun dalam implementasinya transmisi ini sangat dipengaruhi juga oleh keadaan lingkungan. Dengan data rate 54 Mbps biasanya diperoleh *throughput* sebesar 24 Mbps dan dengan data rate 11 Mbps akan diperoleh kecepatan berkisar 5,3 Mbps. Namun demikian, besarnya *throughtput* akan sangat dipengaruhi oleh kualitas dan level sinyal yang sampai ke pengguna WLAN.

Faktor-faktor seperti topologi ruangan, daerah, dan juga cuaca sangat berpengaruh terhadap kualitas sinyal yang digunakan, mengingat sistem transmisi yang digunakan adalah media radio frekuensi. Selain kecepatan, pengaruh gelombang radio juga memberikan dampak terhadap *delay* dari WLAN.

Kelemahan yang lain adalah, harga-harga komponen WLAN dipasaran relatif masih cukup tinggi, sehingga membutuhkan biaya yang besar dan perencanaan yang tepat dan efisien dalam mengimplementasikan WLAN ini. Kapasitas jaringan dari WLAN cukup terbatas mengingat spektrum yang di gunakan juga terbatas, sehingga hal ini akan menimbulkan masalah pada garansi kecepatan dan kualitas transmisi data.

III.5. Jenis-jenis Serangan Pada Wireless LAN

Secara garis besar terdapat beberapa isu keamanan jaringan *wireless* serta resiko pengembangannya yang telah di publikasikan, antara lain serangan terhadap kerahasiaan, integritas data, serta ketersediaan jaringan.

III.5.1. Serangan Pasif *(Passive Attacks)*

Serangan ini biasanya menggunakan akses yang bukan haknya dan tidak melakukan perubahan *content* atau isi paket data. Serangan pasif biasanya berupa penyadapan atau penganalisaan lalu lintas jaringan (*traffic*) yang sering disebut *traffic flow analysis.* Terdapat dua jenis serangan pasif, yaitu:

1. **Eavesdropping**

Merupakan teknik penyerangan yang paling sederhana yang dilakukan oleh seorang penyusup (*intruder*). Hanya dengan sebuah koomputer atau *PDA* yang telah dilengkapi dengan *WLAN card*, penyusup dapat melakukan

passive atacks. *Eavesdropping* menggunakan sebuah alat tau software bernama *snifer* yang dapat mengambil data secara diam-diam tanpa diketahui oleh si korban. Tujuan utama dari *eavesdropping* adalah untuk:

1. Mengetahui siapa saja yang menggunakan jaringan tersebut.
2. Mencari bagian mana saja yang dapat diakses.
3. Mengetahui apa saja kemampuan dari alat-alat yang digunakan di jaringan tersebut.
4. Mengetahui kapan jaringan tersebut dalam keadaan sibuk.

Gambar 3.2. *Eavesdropping*
Sumber : Teknologi *Wireless LAN* dan Aplikasinya, Gunadi, PT. Elex Media Komputindo hal 72.

2. Analisa Traffic

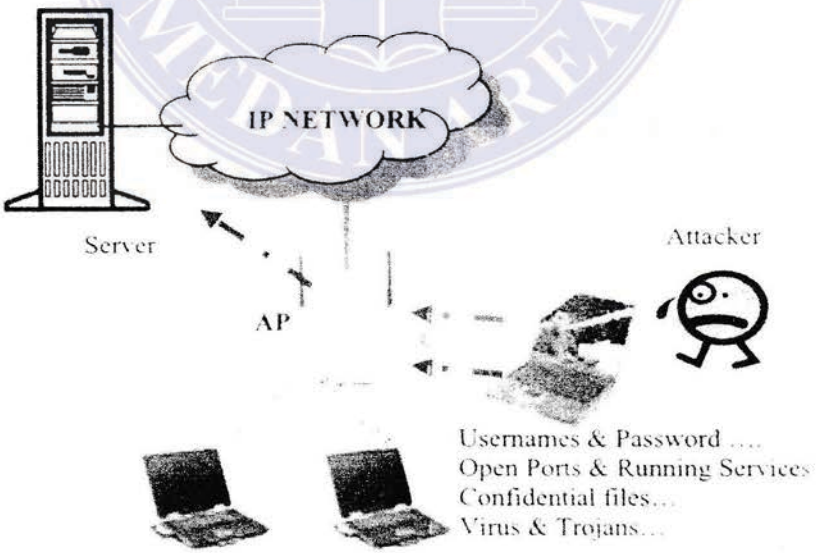
Salah satu jenisnya adalah *wardriving,* di mana penyerang mencari-cari AP yang tersedia. Hal-hal yang diperhatikan dalam pencarian AP ini oleh penyerang adalah mengenai SSID jaringan, dan mencari *address device Media Access Control*. Salain *wardwiring,* analisa yang dilakukan penyerang antara lain mengenai keadaan jaringannya, seperti aktivitas, tipe protokol dan

aktifitas lain yang berguna, seperti ukuran *frame*, data, dan jumlah paket yang terkirim.

III.5.2. Serangan Active (Active Attacks)

Biasanya *active attacks* muncul sebagai lanjutan dari *passive attacks*, di mana data-data yang didapat dari *eavesdropping* digunakan untuk masuk ke dalam jaringan.

active attacks lebih berbahaya di banding dengan *passive attacks*, karena disamping bertujuan untuk masuk ke dalam jaringan WLAN, *attacker* juga akan berusaha mengambil data-data rahasia, bahkan mungkin merusak jaringan. Dampak dari serangan dengan tipe *active attacks* ini tidak terbatas pada jaringan WLAN saja, namun bisa melebar ke seluruh jaringan termasuk *wired* LAN-nya dan kemungkinan dengan tipe serangan ini akan membawa virus yang dapat merusak sistem.



Gambar 3.3. *Active Attacks*
Sumber : Tekonolgi *Wireless LAN* dan Aplikasinya, Gunadi, PT Elex Media Komputindo hal 74.

Terdapat beberapa jenis-jenis serangan *active attacks*, antara lain sebagai berikut:

1. *Unauthorised Access*

Jenis serangan ini dimana penyerang mengikuti atau meniru kerja dari sebuah klien yang sah. Dengan cara kerjanya adalah penyerang melakukan proses *jamming* ke AP dari klien yang sah, sehingga AP tersebut menjadi *non aktif*. Selanjutnya, penyerang membuat sebuah AP tiruan, supaya klien tersebut melakukan autentikasi ke AP tersebut, sehingga penyerang memperoleh semua data yang diperlukan untuk masuk ke dalam jaringan.

2. *Session Hijacking*

Penyerang melakukan pembajakan pada *session* yang dilakukan antara AP dan klien dengan cara menggunakan MAC address dari AP, lalu mengirimkan *frame* yang akan memutuskan koneksi antara AP dengan klien bahwa yang memutuskan koneksi adalah AP, padahal AP sendiri masih melakukan koneksi.

3. *Replay*

Penyerang mengambil paket-paket autentikasi dari sebuah *session* dan mengirimkannya kembali jika ingin membuka sebuah *session*. Karena *session* bersifat *valid*, maka penyerang menggunakan semua otoritas dan file-file penting dari korban.

4. *Client to Client Attacks*

Pada umunya terjadi pada konfigurasi jaringan *Ad Hoc*, dimana penyerang memasuki akses yang ada di komputer korban, lalu mengambil semua data-data yang penting yang terdapat di dalam komputer tersebut.

5. *Infrastruktur Equipment Attacks*

Alat-alat infrastruktur yang tidak terkonfigurasi dengan baik oleh admin jaringan merupakan target utama bagi penyerang untuk memperoleh akses ke dalam jaringan tersebut. Alat-alat jaringan seperti *router, switches, backup servers, dan log servers* merupakan sasaran dari penyerang. Ada beberapa tipe penyerangan pada alat-alat tersebut, namun biasanya dibagi dalam tiga kategori, yaitu *switch attacks, MAC attacks*, dan *routing attacks.*

Tabel 3.4. Perbedaan antara *passive attacks* dengan *active attcks*

Passive Attacks	Active Attacks
Tidak beresiko	Beresiko
Tidak perlu menjadi bagian dari jaringan, karena beberapa WLAN card sudah mensupport mode monitoring, dimana seorang dapat mendengarkan komunikasi tanpa harus menjadi bagian dari jaringan tersebut.	Penyerang terlebih dahulu masuk ke dalam jaringan sebelum melakukan perusakan.
Penyerang hanya dapat mendengar segala aktivitas, namun tidak memainkan jaringan	Penyerang dapat mengacaukan, membajak, dan mengontrol jaringan semaunya.

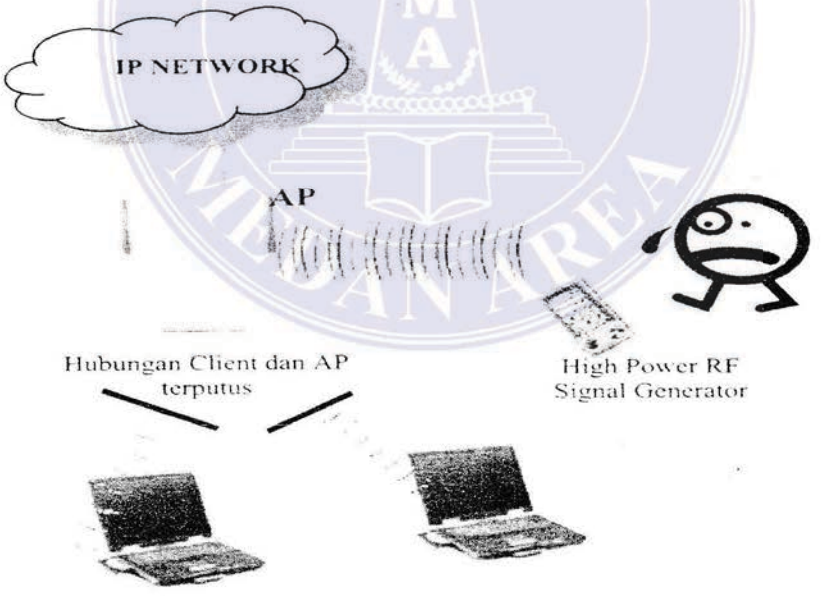
Sumber: Teknologi *Wireless LAN* dan Aplikasinya, Gunadi. PT. Elex Media komputindo hal 78.

III.5.3. *Jamming*

Jamming / Denial of Service Attack (DOS), mudah untuk diterapkan ke dalam jaringan *wireless*. *Jamming* terjadi jika terdapat frekuensi RF saingan yang dapat mengganggu kerja dari *Wireless LAN*. *Jamming* ini dapat terjadi baik disengaja maupun tidak disengaja. *Jamming* yang tidak disengaja biasanya disebapkan adanya alat lain disekitar WLAN, seperti jaringan *cordless phone, bluetooth*, dan lain-lain, yang memili frekuensi kerja yang sama. Hal ini dapat dihindari oleh admin jaringan dengan menerapkan suatu aturan yang melarang keberadaan alat-alat tersebut, sehingga tidak mengganngu kerja WLAN.

Jamming yang disengaja oleh *attacker* biasanya dilakukan dengan membangkitkan suatu frekuensi yang sama dengan frekuensi WLAN dengan daya yang lebih besar daripada daya yang dimiliki WLAN. Dengan demikian, sistem WLAN seolah-olah memiliki *noise* yang besar dari luar dan akibatnya komunikasi antara AP dan klien tidak bisa dilakukan.

Untuk melakukan hal ini, penyerang memerlukan beberapa alat seperti *PDA/notebook* yang sudah di lengkapi dengan *wireless card* untuk mengacaukan trafik WLAN dan *spectrum analyzer* yang akan menentukan pada frekuensi berapakah jaringan tersebut bekerja. Namun tipe penyerangan seperti ini sangat jarang terjadi, mengingat waktu dan biaya yang diperlukan oleh penyerang untuk merusak jaringan yang ada sangat besar.



Gambar 3.4. *Jamming* Jaringan WLAN
Sumber : Teknologi *Wireless LAN* dan Aplikasinya, Gunadi, PT Elex Media Komputindo hal 70.

III.5.4. *Man in The Middle Attacks*

Man in the midle attacks dalam hal ini adalah seseorang *attacker* yang memotong jalur di tengah antara AP dan klien. Pada tipe serangan ini, penyerang menipu klien untuk percaya, bahwa penyerang adalah AP dan juga menipu AP yang sah dari jaringan, bahwa dia adalah klien yang sah. Metode ini menggunakan serangan pada *Address Resolution Protocol (ARP),* yaitu peralatan yang digunakan pada jaringan TCP/IP. *Hacker* dengan peralatan tertentu dapat memamfaatkan AP untuk melakukan control terhadap jaringan *wireless*.

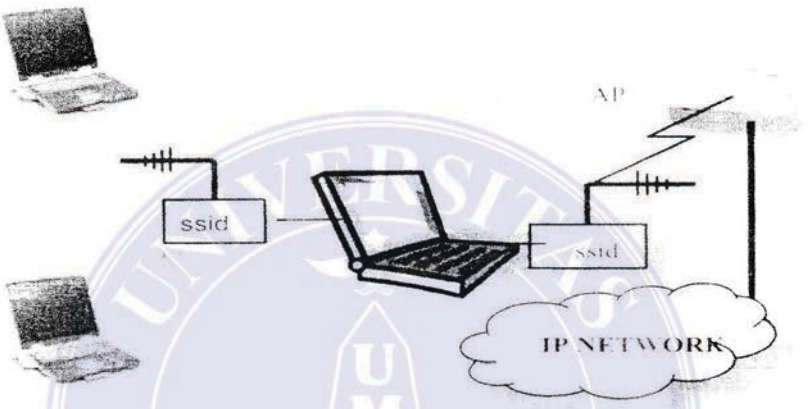
Cara kerja dari tipe penyerang ini lebih kompleks, karena harus menghadapi AP dan klien. Pertama-tama, penyerang berusaha untuk berhubungan dengan AP yang sah dengan cara mengirimkan *request* palsu, dimana AP menganggap bahwa permintaan tersebut palsu, dimana AP menganggap bahwa permintaan tersebut merupakan permintaan dari klien yang sah. Lalu, AP mengirimkan sebuah *challenge* yang nantinya akan dijawab oleh penyerang dengan jawaban yang tepat dan terhubung ke jaringan.

Untuk mencari jawaban ini, penyerang kemudian berganti ke sisi klien. Penyerang seolah-olah akan menjadi AP yang sah bagi klien tersebut. Penyerang mengirimkan *challenge* tersebut ke klien dan klien memberikan jawaban yang tepat. Syarat dari *attacker* tipe ini adalah:

1. Harus mempunyai komputer yang memiliki dua WLAN *card*, satu yang tersambung ke AP yang asli dan yang kedua untuk melayani klien yang pada awalnya tesambung ke AP yang asli tersebut.
2. Mengetahui *ramdom challenge* yang dikirimkan AP yang sah dan juga harus mengetahui jawaban yang tepat.

3. Mempunyai *software* AP yang dipasang di komputer.
4. Sinyal yang diterima dikomputer *attacker* harus lebih besar dari pada yang diterima oleh klien.

Keuntungan bagi *attacker* menggunakan tipe ini di samping memperoleh data yang di inginkan juga akan memperoleh kecepatan yang maksimum.



Gambar 3.5. *Man In the Middle Attacks*
Sumber : Teknologi *Wireless LAN* dan Aplikasinya, Gunadi, PT Elex Media Komputindo hal 80.

BAB V

KESIMPULAN DAN SARAN

V.1. Kesimpulan

Berdasarkan penjelasan yang ada pada bab-bab sebelumnya maka kesimpulan yang dapat di ambil adalah :

1. Wireless LAN merupakan sistem komunikasi data yang dalam pengiriman dan penerimaan data nya dilakukan melalui media udara dengan memamfaatkan radio frekuensi (RF).
2. Pada dasarnya jaringan *Wireless LAN* tidak jauh berbeda dengan jaringan yang menggunakan kabel. Pada jaringan Wireless LAN menggunakan Radio Frekuensi sebagai transmisi datanya sementara pada jaringan kabel menggunakan perangkat kabel untuk melakukan transmisi datanya.
3. Jenis serangan yang paling mengganggu kinerja Wireless LAN adalah jamming. Dimana gangguan tersebut berasal dari jaringan handphone, bluetooth, modem dan notebook.
4. Karena media pengiriman dan penerimaan data nya adalah dengan media udara maka pengamanan data dengan proses Autentikasi di Universitas Medan Area dirasakan sudah aman untuk melindungi *user* dari berbagai kelemahan *Wireless LAN* itu sendiri.

V.2. Saran

1. Posisi penempatan *access point* yang memusat hanya di gedung Biro Rektor membuat layanan koneksi *Wireless LAN* di Universitas Medan Area menjadi lambat. Oleh karena itu Mahasiswa kurang antusias dengan adanya koneksi *wireless* di Universitas Medan Area.
2. Karena Universitas Medan Area menggunakan *Range Closed Office*, seharusnya *access point* lebih baik jangan memusat hanya di gedung Biro Rektor saja, untuk menghindari banyaknnya *overlapping* dan mencegah blank area harus dilakukan penyebaran *access point* ke gedung-gedung lain.
3. Perlunya pengingkatan keandalan jaringan untuk menghindari lemahnya koneksi Wireless LAN, dengan melarang menggunakan peralatan yang dapat mengganggu kinerja Wireless LAN. Misalnya penggunaan modem, bloetooth, dan PDA.

DAFTAR PUSTAKA

Arifin Zaenal. *Sistem Pengaman Bernasis Protokol 802.1x dan Sertfikat*. Yogyakarta: Penerbit Andi.2008.

Arifin Zaenal. *Mengenal Wireless LAN (WLAN)*. Yogyakarta: Penerbit Andi, 2007.

DC Green. *Komunikasi Data*. Yogyakarta: Penerbit Andi, 1995.

Gunadi. *Teknologi Wireless LAN dan Aplikasinya*. Bandung: Elex Media Komputindo, 2005.

Kurniawan Winarsono, *Jaringan Komputer*. Yogyakarta: Penerbit Andi, 2007.

Mulianta.Edi. S. *Pengenalan Protokol Jaringan Wireless Komputer*. Yogyakarta: Penerbit Andi, 2005.

Sugeng Winarno, *Instalasi Wireless LAN*. Bandung: Informatika, 2005

www.google.com/Komputer%20buka%20juga%20http%20_comstp.wordpress.com%20%C2%AB%20Gabriella%27s%20Blog.htm

http://id.m.wikipedia.org/wiki/jaringan_lokal_nirkabel?wasRedirected=true

http://id.m.wikipedia.org/wiki/Bluetooh?wasRedicacted=true

http://id.wikipedia.org/wiki/freukuensi_radio

http://.id.wikipedia.org/wiki/Jaringan_komputer

http://.id.wikipedia.org/wiki/OFDM

www.google.com./komputer/Agni_Lutfi/Blog/sejarah-wireless.html