BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi *wireless* (tanpa kabel) saat ini berkembang sangat cepat seiring dengan kebutuhan informasi yang semakin tinggi. Hal ini disebabkan oleh beberapa faktor yang menjadi keunggulan teknologi *wireless* diantaranya adalah kemampuan komunikasi bergerak, keandalan sistem semakin meningkat, dan biaya pembangunan yang relatif lebih murah dibanding *wireline*.

Teknologi tanpa kabel yang paling populer adalah teknologi *Wireless Local Area Network* (WLAN). Oleh badan IEEE *(Institute of Electrical and Electronic Engineers*) WLAN diberi standar dengan nama 802.11. Pada teknologi WLAN dikenal tiga standar yang paling banyak digunakan di dunia, yaitu IEEE 802.11b, IEEE 802.11g, dan IEEE 802.11a. IEEE 802.11b dan IEEE 802.11g menggunakan frekuensi 2,4 Ghz, sedangkan IEEE 802.11a menggunakan frekuensi 5 Ghz.

Ada dua standar yang diterapkan pada *access point* yaitu 802.11b dan 802.11g. Dengan jarak jangkau 35 meter di dalam ruang (*indoors*) dan sekitar 110 meter pada luar ruangan (*outdoors*). Untuk standar 802.11b mempunyai kecepatan transfer data 11 Mbps. Sedangkan 802.11g bisa mencapai kecepatan transfer data sampai 54 Mbps.

Wireless LAN menggunakan udara sebagai media propagasi. Karena menggunakan udara, jaringan *wireless* berpotensi diakses oleh pengguna yang tidak sah. Hal ini cukup mengganggu pengguna yang lain, dan mengganggu kinerja jaringan secara keseluruhan.

Untuk mengatasi masalah ini, pada *IEEE 802.11* sudah tersedia metode keamanan WEP (*Wired Equivalent Privacy*), namun dalam perkembangannya metode ini sudah tidak banyak digunakan karena masih dapat ditembus oleh pengguna yang tidak sah.

Dengan adanya kondisi diatas, maka diperlukan keamanan jaringan *wireless* yang berlapis-lapis. Karena itu, badan *IEEE (Institute of Electrical and Electronic Engineers*) membentuk standar *802.11i* untuk menciptakan metode keamanan yang lebih baik dari WEP. Metode keamanan baru ini diberi nama *Wi-Fi Protected Access* (WPA).

Kelebihan WPA adalah penggunaan enkripsi data dengan teknik *Temporal Key Integrity Protocol* (TKIP). TKIP mengacak kata kunci menggunakan "*hashing algorithm*" dan menambah *Integrity Checking Feature*, untuk memastikan kunci belum pernah digunakan secara tidak sah. Enkripsi yang digunakan pada WPA adalah RC4 (*Rivest Code 4*).

Terdapat dua jenis WPA (*Wi-Fi Protected Access*) yaitu WPA dan WPA2. Perbedaan diantara WPA dan WPA2 adalah pada jenis enkripsinya. Enkripsi yang digunakan pada WPA2 adalah AES (*Advanced Encryption Standard*). *RC4* dan *AES* merupakan jenis algoritma simetrik, yaitu algoritma yang menggunakan kunci enkripsi yang sama dengan kunci deskripsinya.

Selain penggunaan enkripsi diatas, pengguna juga dilindungi dengan autentikasi melalui *Pre Shared Key* (PSK). *Pre Shared Key* adalah proses pencocokan identitas dengan menggunakan kunci yang sama antara *Access Point* dan *client*.

Dari uraian tersebut, dalam skripsi ini pembahasan yang dilakukan adalah mengkaji proses enkripsi dan autentikasi pada WPA-PSK (*Wi-Fi Protected Access-Pre Shared Key*) dan WPA2-PSK (*Wi-Fi Protected Access2-Pre Shared Key*) serta pengaruhnya terhadap kinerja jaringan WLAN. Perhitungan yang dilakukan adalah perhitungan *delay time* dan *throughput* dari masing-masing metode keamanan, untuk kemudian dibandingkan dan diambil kesimpulan. Hasil yang didapatkan untuk kedepannya diharapkan dapat memudahkan pengguna dalam menentukan pilihan metode keamanan yang akan digunakan.

1.2 Rumusan Masalah

Sesuai dengan latar belakang yang telah dijelaskan diatas, maka dapat ditentukan rumusan masalah sebagai berikut :

1. Bagaimana proses enkripsi dan autentikasi WPA-PSK dan WPA2-PSK pada *Wireless Local Area Network*?
2. Bagaimana model penerapan WPA-PSK dan WPA2-PSK pada *Wireless Local Area Network*?
3. Bagaimana pengujian enkripsi untuk keamanan data menggunakan WPA-PSK dan WPA2-PSK?

4. Bagaimana pengaruh penerapan WPA-PSK dan WPA2-PSK pada *Wireless Local Area Network* berdasarkan *delay time* dan *throughput?*

1.3 Ruang Lingkup

Berdasarkan rumusan masalah yang ada, maka dalam mengkaji penerapan WPA-PSK dan WPA2-PSK pada jaringan WLAN, diambil ruang lingkup sebagai berikut :

1. Standar jaringan yang digunakan adalah standar IEEE 802.11b
2. Penerapan enkripsi data menggunakan RC4 dan AES dilakukan dengan menggunakan program simulasi.
3. Kriteria aman yang digunakan adalah data aman jika data tidak bisa dibaca oleh penyadap.
4. Data yang digunakan adalah dalam bentuk teks.

1.4 Tujuan

Penulisan skripsi ini bertujuan untuk mengkaji penerapan WPA-PSK dan WPA2-PSK pada jaringan WLAN.

1.5 Kontribusi

Dengan penelitian ini diharapkan dapat memberi kontribusi dalam beberapa hal, antara lain :

1. Setelah membaca skripsi ini, pengguna jaringan *wireless* memiliki pengetahuan yang cukup tentang cara kerja, kelebihan dan kekurangan, serta penerapan metode keamanan WPA-PSK dan WPA2-PSK.
2. Dapat memberikan kontribusi untuk pengembangan lebih lanjut teknologi *wireless* yang ada sekarang.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini adalah sebagai berikut :

Bab I: Pendahuluan

Berisi latar belakang, rumusan masalah, ruang lingkup, tujuan, kontribusi, dan sistematika penulisan.

Bab II: Dasar Teori

Menjelaskan tentang jenis-jenis konfigurasi jaringan *wireless*, standarisasi menurut IEEE 802.11, konfigurasi jaringan wireless LAN, serta perhitungan *delay time* dan *throughput* pada jaringan *wireless*. Menjelaskan mekanisme enkripsi dan autentikasi pada jaringan *wireless* LAN, serta sistem keamanan WPA-PSK dan WPA2-PSK.

Bab III: Metodologi

Menjelaskan tentang langkah-langkah yang dilakukan dalam rangka menyelesaikan penulisan skripsi ini.

Bab IV: Pembahasan dan Hasil

Berisi analisis penerapan WPA-PSK dan WPA2-PSK pada jaringan *Wireless* LAN.

Bab V: Penutup

Berisi kesimpulan dan saran berdasarkan analisis yang telah dilakukan.