PEMODELAN PROTOKOL OTENTIKASI W*IRELESS LOCAL AREA NETWORK* DENGAN UML

Heri Suroyo
Departemen Teknik Informatika, Fakultas Ilmu Komputer,
Universitas Binadarma Palembang
Jl. A Yani No12 Palembang, 30264
Telpon : 0711 515679, Fax : 0711 515582
E-mail : herisuroyo@binadarma.ac.id

Abstrak

Tulisan ini memfokuskan pada pemodelan protokol otentikasi Wireless Local Area Network (WLAN). Latar belakang dari paper ini adalah perlunya pemodelan dalam menjelaskan teori model otentikasi WLAN. Terdapat 3 (tiga) model otentikasi WLAN yang akan diuraikan yaitu Model otentikasi terbuka, otentikasi kunci bersama, dan otentikasi dengan RADIUS.Metode penelitian yang digunakan adalah narative research. Sedangkan pemodelan protokol dilakukan dengan bahasa Unified Modeling Language (UML). Manfaat dari kajian model otentikasi WLAN ini setidaknya ada dua. Pertama, bisa digunakan untuk menjelaskan perbedaan antar model otentikasi misalnya dari sisi keamanan. Kedua, bisa menjadi bahan pertimbangkan saat akan mengimplementasikan otentikasi WLAN yang akan dipakai dalam membangun jaringan komputer.

Kata Kunci: pemodelan, protokol otentikasi, WLAN, dan UML.

Abstract

This paper focuses on modeling the authentication protocol of Wireless Local Area Network (WLAN). The background of this paper is the need for modeling in explaining the theoretical model of WLAN authentication. There are three (3) WLAN authentication models that will describe the model open authentication, shared key authentication, and authentication with RADIUS. Metode study is a narrative research. While the protocol is done with language modeling Unified Modeling Language (UML). The benefits of this study WLAN authentication models are at least two. First, it can be used to explain the differences between the model examples of the security authentication. Secondly, could be material to consider when implementing a WLAN authentication that will be used in building computer networks.

Keywords: modeling, authentication protocols, WLAN, and UML.

1. PENDAHULUAN

Metode otentikasi yang digunakan dalam perancangan Wi-Fi menentukan faktor keamanan Wi-Fi. Pada lingkungan nirkabel, dimana akses jaringan tidak dapat dibatasi oleh parameter fisik, kerangka keamanan harus menyediakan otentikasi akses jaringan. Hal ini penting karena pada prinsipnya data yang ditransmisikan dalam jaringan tidak boleh dibaca oleh siapapun kecuali pengguna (*user/client*) yang terhubung dengan jaringan. Namun mengingat kompleksitas teori dan banyaknya metode dalam implementasi otentikasi WLAN maka diperlukan sebuah metode pemodelan pada saat perancangan sistem. Hal ini karena tidak mudah menjelaskan tentang pentingnya otentikasi pada arsitektur keamanan jaringan ini terutama bagi mahasiswa atau pengguna hotspot [4].

Sebelum WLAN diimplementasikan sebagai sistem jaringan pada suatu perusahaan atau lembaga, diperlukan perencanaan dan pengembangan sistem dengan beberapa tahapannya. Pemodelan diperlukan untuk menggambarkan dan mengkomunikasikan secara sederhana agar sistem dapat dipahami dan dikoreksi [8].

UML adalah bahasa pemodelan dengan tujuan umum. Protokol jaringan adalah contoh yang sangat bagus untuk dilakukan pemodelan dengan UML. UML menyediakan kemampuan untuk mengeksekusi dan memvisualisasikan perilaku sistem dari model desain [6]. Sementara pendapat lain mengatakan saat ini UML telah menjadi standar pemodelan. Hal ini terutama karena UML merupakan bahasa pemodelan untuk keperluan umum tanpa semantik formal. Dari beberapa referensi diatas kiranya cukup menjadi dasar bagi Permasalahan utama dalam penelitian ini adalah bagaimana menggambarkan model protokol otentikasi WLAN dengan UML. Sedangkan tujuan penelitian ini adalah Melakukan pemodelan pada 3 model protokol otentikasi WLAN dengan bahasa pemodelan UML. Sementara manfaat penelitian yang akan diperoleh dari penelitian adalah sebagai berikut : 1) Bagi dosen pengajar

matakuliah jaringan komputer akan membantu dalam menjelaskan tentang teori protokol otentikasi WLAN. 2) Bagi pengembang jaringan bisa menjadi bahan pertimbangkan saat akan mengimplementasikan otentikasi WLAN yang akan dipakai dalam membangun jaringan komputer.

2. STUDI PUSTAKA

a. Pengertian Jaringan WLAN

Wireless LAN (WLAN atau WiFi) adalah sistem transmisi data dengan gelombang radio yang didesain untuk menyediakan akses jaringan dengan spesifikasi standar 802.11 dari IEEE, sedangkan pengertian Wi-Fi adalah berasal dari Wi-Fi Alliance yaitu lembaga pembuat sertifikasi pada peralatan Wi-Fi yang menjamin pengoperasiannya. Standar 802.11 selesai pada 1997 dan pada tahun 1999 dibuatlah standar internasionalnya[7].

b. Model Protokol Otentikasi Jaringan WLAN

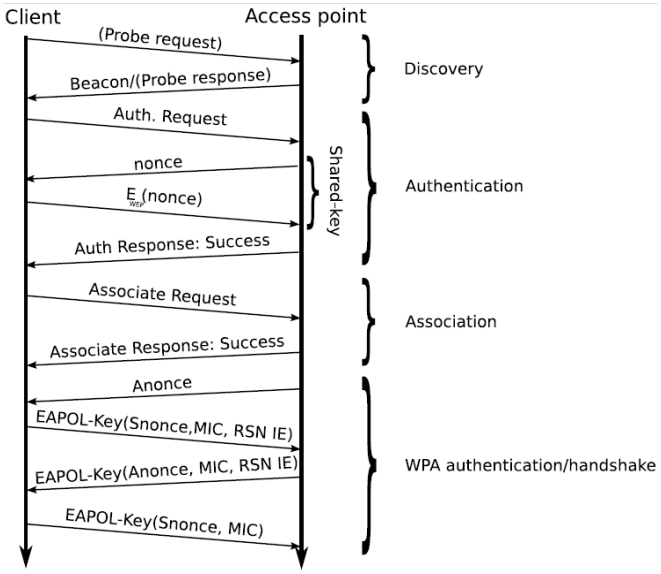
Pengertian otentikasi adalah hanya klien yang tahu kunci rahasia bersama dapat terhubung ke jaringan[3]. Ada tiga model otentikasi WLAN yaitu:

1. Otentikasi Terbuka.

   Sesuai namanya, sistem otentikasi terbuka mengotentikasi siapapun yang melakukan permintaan proses otentikasi dengan *access point*.

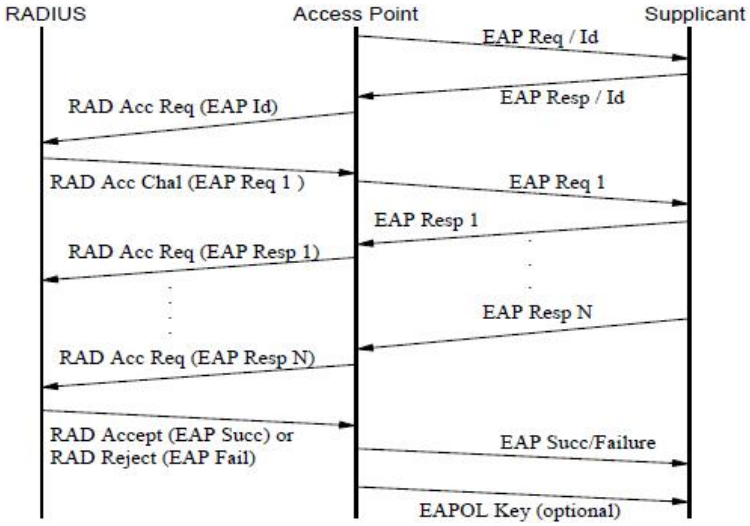
2. Otentikasi dengan Kunci Bersama.

   Otentikasi kunci bersama menggunakan tantangan standar dan respon bersama dengan kunci rahasia bersama untuk menyediakan otentikasi[3].



Gambar 1. Protokol koneksi jaringan Wi-Fi.[3]

3. Otentikasi berbasis *RADIUS Server*.
   RADIUS (*Remote Authentication Dial-In User Service*) merupakan metode yang dianggap mudah diimplementasikan, sederhana dan efisien. RADIUS adalah sebuah network *protokol otentikasi WLAN* yang digunakan untuk membuat manajemen akses secara terkontrol pada sebuah jaringan yang besar, protokol membawa paket data yang ter*encapsulation* didalam paket data tersebut. RADIUS dikembangkan dipertengahan tahun 1990 oleh *Livingstone Enterprise* (sekarang *Lucent Technologies*). *Port* yang dipakai RADIUS adalah *port* 1812 yang format standarnya ditetapakan pada *Request for Command* (RFC) 2138 [1]. Untuk membangun hotspot dengan otentikasi RADIUS bisa menggunakan aplikasi Chilispot, chillispot memerlukan beberapa infrastruktur yaitu: 1. Koneksi internet, 2. Wireless LAN Access Point, 3. Radius Server, 4. Database Server[1].



Gambar 2. Sebuah sesi otentikasi 802.1X lengkap tentang pesan EAP dan RADIUS[4].

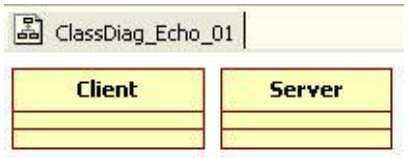
c. **Penelitian Relevan Sebelumnya.**

Penggunaan UML untuk pemodelan protokol diantaranya bisa diterapkan dalam model protokol ECHO pada komunikasi *client-server*. Protokol ECHO memiliki karakteristik sebagai berikut[8]:

1) Ada dua entitas yang berkomunikasi: Klien dan Server,
2) Klien mengirimkan satu pesan *"Halo"* untuk dijawab Server dan Server membalas dengan pesan *"Hello_ACK",*
3) Proses komunikasi selesai. Protokol tersebut bisa dijelaskan perilakunya dengan menggunakan diagram UML seperti nampak pada gambar berikut.

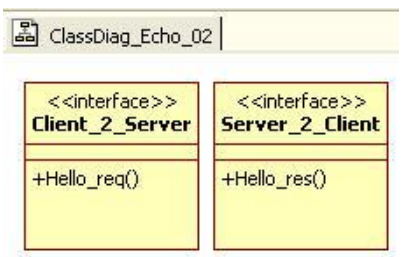
Gambar 3. Diagram Komunikasi Protokol Jaringan Client-Server.

Dari diagram nampak ada 2 objek dan relasi yang meng-hubungkan antara dua objek tersebut. Dalam UML objek-objek tersebut diimplementasikan dalam kelas-kelas. Kita dapat meng-gunakan *Class Diagram* untuk menggambarkan kelas-kelas sederhana tersebut seperti gambar berikut :



Gambar 4. Diagram Client *dan* Server

Dalam konteks protokol, kita dapat mengelompokkan pesan-pesan komunikasi ke dalam kelompok-kelompok yang mewakili arah *Sender-Receiver*. Setiap kelompok dapat diwakili oleh Interface. Dalam hal ini, kita dapat membuat dua antarmuka: *Client_2_Server* dan *Server_2_Client*. Antarmuka pertama berisi pesan *Hello_req* sedangkan antarmuka kedua berisi *Hello_res*. Dengan demikian kita dapat menggambarkan kedua kelas yang lengkap beserta *method*-nya seperti gambar berikut :

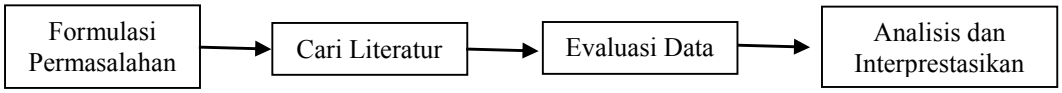


Gambar 5. Pemodelan Class Diagram kelas Client dan Server

Selanjutnya dengan diagram komponen, diagram sequence, dan diagram aktivitas digunakan untuk memodelkan perilaku dari model protokol otentikasi.

3. METODOLOGI PENELITIAN

Metode yang digunakan dalam penelitian ini adalah metode *narative research,* yaitu dengan meng-*capture* berbagai pendapat pakar yang langkah-langkahnya bisa digambarkan sebagai berikut [2]:



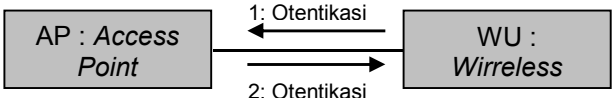
Gambar 6. Langkah-langkah Metode Narative Research

4. HASIL PENELITIAN

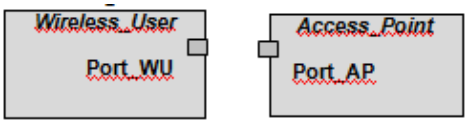
[1] Pemodelan Protokol Otentikasi Terbuka (*Open Authentication*).

Komunikasi yang terjadi pada otentikasi terbuka bisa dilihat dari protokol otentikasinya yaitu:

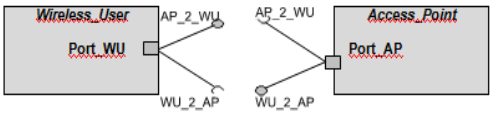
1) Proses otentikasi dimulai dengan *wireless user* mengirimkan pesan *open system authentication request*, yang mengandung informasi mengenai *MAC Address* sebagai alamat asal.
2) *AP* membalas pesan yang diterima dari *wireless user* dengan mengirimkan pesan *open system authentication response.*
3) Otentikasi selesai dan berhasil/gagal. Perilaku dari protokol tersebut dengan UML bisa digambarkan melalui langkah-langkah sebagai berikut.



Gambar 7. Diagram Komunikasi Protokol Otentikasi Terbuka.

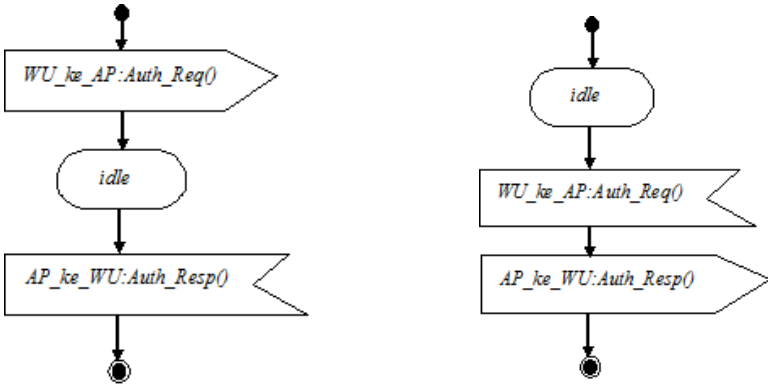


Gambar 8. Komponen Diagram Objek AP dan WU



Gambar 9. Pemodelan untuk menghubungkan WU dan AP pada component diagram.

Penggambaran perilaku masing-masing node dalam menghasilkan pertukaran pesan yang diharapkan dengan Diagram Aktivitas atau *State Machine Diagram*. Pertama model Diagram Aktifitas untuk node *WirelessUser* dan dari arah sebaliknya yaitu dari aktifitas pada node *AccessPoint* adalah sebagai berikut:

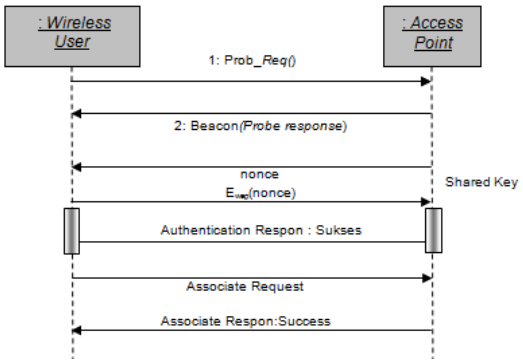


(a) Aktivitas komunikasi dari WU ke AP (b) Dari AP ke WU

Gambar 10. Diagram Aktivitas komunikasi dari WU ke A dan sebaliknya.

[2] Pemodelan Protokol Otentikasi Kunci Bersama (*Shared Key Authentication*).

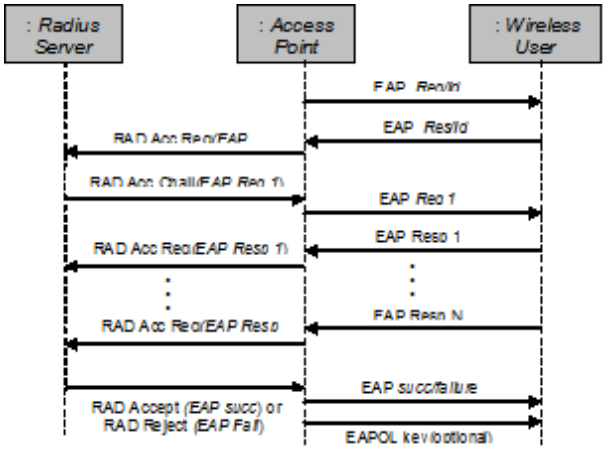
Otentikasi kunci bersama merupakan tambahan fitur dalam WPA. Objek pada pemodelan otentikasi kunci bersama sama dengan otentikasi terbuka yaitu *WU* atau *Client* dan *AP*. Perbedaannya adalah pada perilakunya yang lebih dikembangkan. Berikut ini penggambaran dengan diagram *sequence*.



Gambar 11. Diagram Sequence Shared Key Authentication

[3] Pemodelan Otentikasi Berbasis *RADIUS Server*.

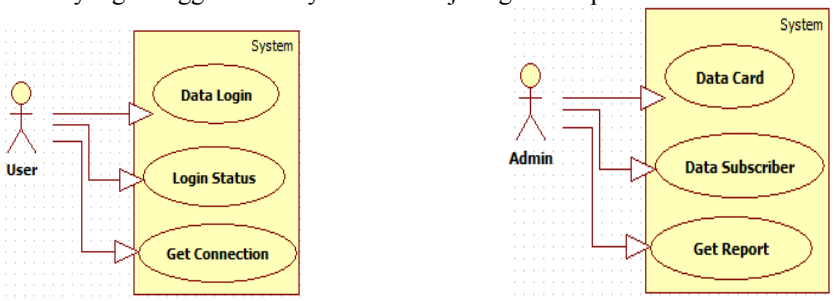
Untuk menggambarkan sesi otentikasi 802.1X lengkap yang menunjukkan pesan EAP dan RADIUS bisa digambarkan dengan diagram sequence. Proses otentikasi terjadi dengan melalui empat tahap, yang disebut *four way handshake*. Sequence Diagram pada otentikasi dengan RADIUS menggambarkan alur protokol komunikasi yang terjadi. antara tiga objek entitas yaitu *Server Radius*, *Access Point* dan *Wirreless User*.



Gambar 12. Diagram Sequence Otentikasi berbasis RADIUS

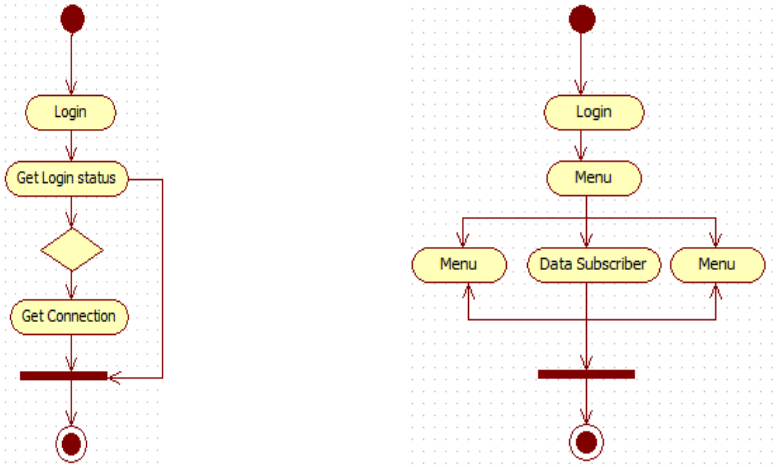
Pada tahap perancangan Otentikasi berbasis *RADIUS Server* pemodelan hubungan antara entitas luar dengan sistem bisa digambarkan dengan diagram Use Case. Terdapat 2 (dua) entitas luar pada sistem ini, kedua entitas tersebut adalah:

1. *User*, User adalah user yang menggunakan layanan dalam jaringan komputer *wireless*.



(a) Pengguna *(b) Administrator*

Gambar 13. Diagram Use Case



(a) Aktivitas *User* (b) Aktivitas *Admin*

Gambar 14. Activity Diagram Pengguna dan Administrator

5. KESIMPULAN DAN SARAN

1) Pemahaman tentang perbedaan ketiga model protokol otentikasi WLAN menjadi lebih jelas dengan digambarkan melalui UML.

2) Dengan UML Model Protokol otentikasi dengan RADIUS tergambar sebagai model protokol yang lebih menjamin keamanan koneksi WLAN.

3) Saran dalam penelitian ini adalah diperlukan penelitian lebih lanjut untuk mengetahui pengaruh protokol otentikasi WLAN yang digunakan terhadap efektivitas dan kinerja pengguna.

6. DAFTAR PUSTAKA

[1] C. Rigney, S. Willens, A. Rubens, W. Simpson, 2008, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138.
[2] Hasibuan, Zainal A, 2007, *Metodologi Penelitian pada Bidang Ilmu Komputer dan Teknologi Informasi,* Fakultas Ilmu Komputer Universitas Indonesia.
[3] Helleseth, 2006, *Wi-Fi Security How to Break and Exploit*, Thesis for the Degree Master of Science Department of Informatics University of Bergen.
[4] Minho Shin, Arunesh Mishra, William A. Arbaugh Justin Ma, 2006, Wireless Security and Internetworking. *The Proceedings of IEEE on Cryptography and Security*, Vol.94, No.2, pp 455–466, (SCI: impact factor 4.613)
[5] Nico de Wet and Pieter Kritzinger,2009, *Using UML Models for the Performance Analysis of Network Systems*, Department of Computer Science University of Cape Town
[6] Sandra Smith, Alain Beaulieu and W. Greg Phillips,2008, *Modeling Security Protocols Using UML 2*, Department of Electrical and Computer Engineering Royal Military College of Canada.
[7] Tharom, T., Onno W.P, 2001, "*Teknologi VoIP*", Jakarta, PT.Elex MediaKomputindo.
[8] Setyo Wawan W,2008, *Pemodelan VoIP dengan menggunakan UML*, Teknik Elektro UNDIP.
[9] ISTE Publishing Knowledge Wiley, 2014. Availlable at : http://www.iste.co.uk/index.php?p=a&ACTION=View&id=420, Mei.
[10] OMG Object Management Grouph, 2013 Availlable at : http://www.omg.org/spec/UML/2.1.2/Superstructure/PDF