UNIVERSITAS INDONESIA

PENGEMBANGAN DAN UJI KINERJA SISTEM PENDETEKSI *ROGUE ACCESS POINT* MENGGUNAKAN APLIKASI BERBASIS WEB DENGAN METODA PENGUKURAN WAKTU ROUND TRIP TIME

TESIS

MUHAMAD FARID ABDILLAH

NPM. 0906578043

FAKULTAS TEKNIK

PROGRAM STUDI TEKNIK ELEKTRO

DEPOK

JUNI 2011

HALAMAN PERNYATAAN

ORISINALITAS

Tesis ini adalah hasil karya saya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar.

Nama : Muhamad Farid Abdillah

NPM : 0906578043

Tanda Tangan :

Tanggal : 13 Juni 2011

HALAMAN PENGESAHAN

Tesis ini diajukan oleh :
Nama : Muhamad Farid Abdillah, ST.
NPM : 0906578043
Program Studi : Teknik Elektro
Judul Tesis : Pengembangan Dan Uji Kinerja Sistem Pendeteksi Rogue Access Point Menggunakan Aplikasi Berbasis Web Dengan Metoda Pengukuran Waktu Round Trip Time

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Teknik pada Program Studi Teknik Elektro, Fakultas Teknik, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing : Prof. Dr.-Ing. Ir. Kalamullah Ramli, M.Eng. ( )

Penguji : Prof. Dr. Ir Riri Fitri Sari, M.Sc, MM ( )

Penguji : Dr. Ir. Anak Agung Putri Ratna, M.Eng ( )

Penguji : Prima Dewi Purnamasari, ST., MT., MSc ( )

Ditetapkan di : Depok

Tanggal : Juli 2011

UCAPAN TERIMA KASIH

Puji syukur saya panjatkan kepada Allah SWT karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan tesis ini. Penulisan tesis ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Magister Teknik, Program Studi Teknik Elektro, kekhususan Teknik Jaringan Informasi dan Multimedia, Fakultas Teknik, Universitas Indonesia. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan tesis ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

(1) Prof. Dr.-Ing. Ir. Kalamullah Ramli, M.Eng. dan Muhammad Salman S.T., MIT, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan tesis ini;
(2) orang tua, keluarga besar, serta istri dan anak-anak saya yang telah memberikan bantuan dukungan moral dan material;
(3) dan sahabat-sahabat saya yang telah banyak membantu saya dalam menyelesaikan tesis ini.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga tesis ini membawa manfaat bagi pengembangan ilmu.

Depok, 13 Juni 2011

Penulis,

Muhamad Farid Abdillah
NPM. 0906578043

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Muhamad Farid Abdillah
NPM : 0906578043
Program Studi : Jaringan Komunikasi Dan Multimedia
Departemen : Teknik Elektro
Fakultas : Teknik
Jenis karya : Tesis

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :
"Pengembangan Dan Uji Kinerja Sistem Pendeteksi Rogue Access Point Menggunakan Aplikasi Berbasis Web Dengan Metoda Pengukuran Waktu Round Trip Time"
beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia / formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mepublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis / pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 15 Juni 2011
Yang menyatakan

(Muhamad Farid Abdillah)

ABSTRAK

Nama : Muhamad Farid Abdillah

Program Studi : Teknik Elektro

Judul : **PENGEMBANGAN DAN UJI KINERJA SISTEM PENDETEKSI ROGUE ACCESS POINT MENGGUNAKAN APLIKASI BERBASIS WEB DENGAN METODA PENGUKURAN WAKTU ROUND TRIP TIME**

Pembimbing : Prof. Dr.-Ing. Ir. Kalamullah Ramli, M.Eng.

Salah satu gangguan keamanan jaringan yang ada pada teknologi *Wifi* adalah adanya perangkat *Rogue Access Point (*RAP*)*, yang merupakan *Access Point* yang tidak dilegitimasi oleh administrator jaringan. Deteksi terhadap keberadaan RAP sudah banyak dikembangkan dengan berbagai metoda. Salah satunya adalah deteksi RAP menggunakan aplikasi berbasis web yang tidak memerlukan asistensi dari administrator jaringan. Sistem ini menggunakan waktu *Round Trip Time* dari *DNS lookup* dan *DHCP request* sebagai parameter untuk mendeteksi keberadaan RAP. Hasil pengujian menunjukkan bahwa pada RAP diperoleh *RTT DNS* lebih lama dibandingkan *RTT DHCP* sebagai konsekuensi adanya hop tambahan. Tingkat akurasi sistem dipengaruhi oleh trafik pada RAP dan beban pada *legitimate* AP, semakin tinggi trafik pada RAP dan beban pada AP semakin berkurang keakuratan sistem. Implementasi sistem berhasil dilakukan dengan tingkat akurasi pendeteksian sistem mencapai 98,2% pada kondisi trafik idle, kemudian menurun menjadi sekitar 88,9% pada kondisi trafik medium dan turun lagi menjadi sekitar 70,3% pada kondisi trafik tinggi.

Kata kunci*: WirelessLAN, Access Point,* Keamanan Jaringan, *Rogue Access Point,* RAP*, RTT.*

ABSTRACT

Name : Muhamad Farid Abdillah

Study Program : Teknik Elektro

Title : **DEVELOPMENT AND PERFORMANCE EVALUATION OF ROGUE ACCESS POINT DETECTION SYSTEM USING WEB BASED APPLICATION WITH ROUND TRIP TIME MEASUREMENT METHOD**

Supervisor : Prof. Dr.-Ing. Ir. Kalamullah Ramli, M.Eng.

Rogue Access Point (RAP) is one of the vulnerabilities in Wifi technology, which is an Access Point that is not legitimated by the network administrator. The detection of RAP has been developed widely with various methods. A Method that has been developed in this study is the RAP detection using web based aplication which does not require network administrator assistant. This system uses Round Trip Time of DNS lookup and DHCP request as parameters that will be used for detecting the existence of RAP. The test shows that on RAP the DNS RTT will be longer than the DHCP RTT as the consequensies of the addition of hop. The system's accuracy is influenced by the WiFi traffic and load on legitimate AP, the bigger the traffic and the load make the system's accuracy more decreased. The system accuration level is 98,2% on idle traffic, decrease to 88,9% when the traffic is medium and become 70,3% on high traffic condition.

Keywords: WirelessLAN, Access Point, Network *security*, Rogue Access Point, RAP, RTT

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

AP	Access Point
DNS	Domain Name Service
GPL	GNU General Public License
GUI	Graphical User Interface
HDT	Hop Differentiating Technique
IAT	Inter Arrival Time
MITM	Man In The Middle
MAC	Medium Access Controller
RAP	Rouge Access Point
RC4	Rivest Cipher 4
RDMS	Relational Database Management System
RTT	Round Trip Time
SSID	Service Set Identifier
SPRT	Sequential Probability Ratio Test
SQL	Structured Query Language
TMM	Trained Mean Matching
WEP	Wired Equivalent Privacy
WIFI	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wifi Protected Access

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Kemudahan dalam mengakses internet dengan menggunakan jaringan wireless berimplikasi terhadap kemungkinan terjadinya gangguan keamanan jaringan. Pada umumnya resiko yang sering terjadi pada jaringan nirkabel adalah tidak adanya konfidentialitas – yakni *user* yang tidak terotorisasi dapat mengakses kedalam sistem dan memperoleh informasi; serta tidak adanya integritas data – dikarenakan data yang ada dalam jaringan dapat diubah sehingga masih banyak perusahaan dan instansi pemerintah yang tidak mengijinkan jaringan wireless dipakai sebagai media akses bagi para pegawainya [1].

Banyaknya layanan *Access Point* yang disediakan untuk mengakses internet selain memudahkan *user* dalam mencari informasi di internet ternyata juga memberikan kekhawatiran bagi *user* sendiri apakah *Access Point* yang dipakai tersebut memang *Access Point* yang disediakan oleh service provider atau merupakan *Access Point* yang dibuat oleh orang yang memiliki kepentingan untuk mencuri informasi menggunakan bantuan *Access Point* yang ilegal. Hal ini dikarenakan tidak mudah bagi *user* yang memiliki keterbatasan literasi komputer/network untuk membedakan antara *Access Point* yang sesungguhnya dengan *Access Point* ilegal tanpa menggunakan perangkat keras / lunak khusus yang didesain untuk mendeteksi keberadaaan *Access Point* ilegal tersebut. *Access Point* ilegal atau yang tidak memiliki legitimasi dari administrator / service provider inilah yang kemudian disebut dengan istilah *Rogue Access Point (* RAP*)*. Perangkat keras/lunak yang digunakan untuk mendeteksi keberadaan RAP pada umunnya menggunakan 3 macam pendekatan. Pertama menggunakan Pendekatan wireless, Pendekatan Wired, dan Pendekatan Hybrid. Dari ketiga pendekatan tersebut sebagian besar deteksi RAP dilakukan dengan melibatkan peran dari administrator jaringan dan memerlukan *deployment* perangkat deteksi RAP kedalam infrastruktur jaringan yang akan dideteksi. Sedangkan deteksi RAP yang tidak melibatkan melibatkan peran dari administrator jaringan dan tidak memerlukan *deployment* perangkat deteksi RAP kedalam infrastruktur jaringan

yang akan dideteksi belum banyak dikembangkan, hal inilah yang menarik perhatian penulis sehingga tertarik untuk mengembangkannya.

Dalam penelitian ini akan dikembangkan sistem online yang dapat membantu *user* terutama *novice user* untuk mendeteksi keberadaaan *Rogue Access Point*. Hal ini dirasa perlu mengingat selama ini sebagian besar *user* yang menggunakan Akses Point tidak mengetahui *Access Point* yang digunakannya merupakan *Rogue Access Point* atau tidak tanpa asistensi dari administrator jaringan, hal ini dikarenakan sebagian besar solusi yang ditawarkan untuk mendeteksi RAP oleh peneliti atau vendor komersial masih terfokus pada infrastruktur jaringan *Wireless LAN* yang melibatkan peran administrator jaringan. Meskipun ada juga *user* yang dapat mendeteksi keberadaan RAP tanpa asistensi administrator jaringan namun diperlukan Perangkat Lunak atau *tool-tools* khusus yang harus digunakan *user* sehingga hal ini tidaklah mudah bagi *novice user* pada umumnya.

Sepanjang pengetahuan penulis sistem yang dikembangkan penulis merupakan sistem online pertama yang digunakan untuk mendeteksi RAP tanpa melibatkan asistensi administrator jaringan dengan menggunakan algoritma metoda pengukuran waktu RTT [2] yang digunakan peneliti sebelumnya untuk skema pendeteksian RAP secara independen yang diimplementasikan pada sisi *end user*, sehingga ini merupakan kontribusi utama.

1.2. Tujuan Penulisan

Tujuan dari penulisan penelitian ini adalah implementasi sistem untuk membantu *user* terutama *novice user* untuk melakukan pendeteksian *Rogue Access Point* menggunakan aplikasi berbasis web berdasarkan metoda pengukuran waktu pengiriman paket data atau *Round Trip Time (RTT)*, sehingga keamanan informasi dan privasi dari *user* dapat terjaga.

1.3. Batasan Masalah

Permasalahan yang akan dibahas pada tesis ini dibatasi pada metoda deteksi RAP yang terhubung secara wireless kedalam jaringan melalui Akses Point yang menggunakan interkoneksi kabel ke gateway / router untuk koneksi ke

internet. Untuk Akses Point yang menggunakan interkoneksi ke internet menggunakan wireless akses tidak dicakup dalam penelitian ini dikarenakan ada ketidaksesuaian antara algoritma yang dipakai peneliti dengan topologinya.

1.4. Sistematika Penulisan

Pembahasan yang dilakukan pada penelitian ini meliputi empat bab, yaitu:

Bab 1 Pendahuluan

Bagian ini terdiri dari latar belakang masalah, tujuan penelitian, batasan masalah dan sistematika penulisan.

Bab 2 *Rogue Access Point*

Bagian ini berisi tinjauan umum mengenai Wireless *Security*, tinjauan umum *Rogue Access Point*, Prinsip Deteksi *Rogue Access Point*, dan Prinsip Deteksi *Rogue Access Point* Dengan Metoda Pengukuran waktu.

Bab 3 Perancangan Sistem Deteksi *Rogue Access Point* Berbasis Web

Pada Bab ini berisi penjelasan mengenai skenario pendeteksian *Rogue Access Point* menggunakan aplikasi berbasis web berdasarkan metoda pengukuran waktu RTT serta implementasi dari sistem.

Bab 4 Implementasi dan Pengujian

Pada bagian ini dibahas mengenai implementasi dari sistem kemudian dilanjutkan dengan pengujian terhadap sistem pada beberapa skenario yang disiapkan, serta berisi mengenai analisa dari data yang diperoleh dari pengujian sistem tersebut.

Bab 5 Kesimpulan

Bagian ini berisikan kesimpulan dari hasil implementasi dan pengujian sistem pendeteksi rogue AP berbasis Web ini.

BAB 2
ROGUE ACCESS POINT

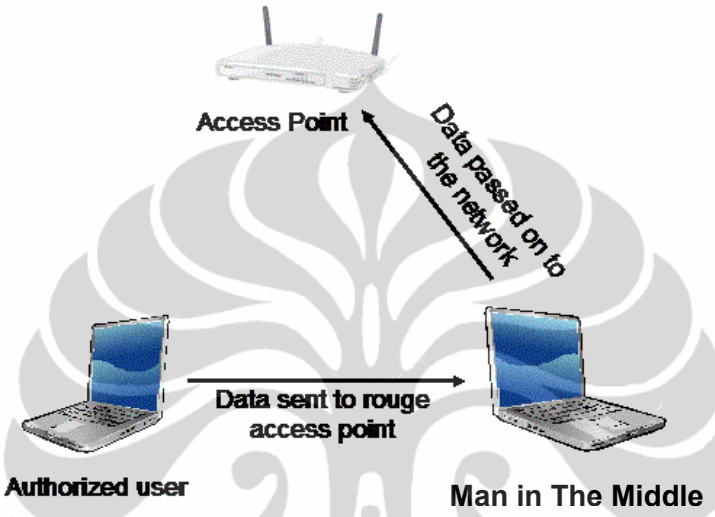
2.1. KEAMANAN *WIRELESS LAN*

Pada umumnya terdapat kesamaan celah keamanan yang dapat terjadi pada jaringan IP yang terkoneksi secara kabel ataupun nirkabel, yaitu keduanya dapat mengalami gangguan keamanan dari tingkat yang paling rendah sampai pada tingkat yang mengakibatkan kerugian yang cukup signifikan. Namun yang membedakan adalah sifat *Wifi* yang selalu mem-*broadcast* pada layer fisiknya keseluruh arah sehingga mempermudah terjadinya akses pada layer fisik dibandingkan pada jaringan kabel.

Pada *Wifi* seorang *user* dimungkinkan untuk melakukan pengendusan paket yang ditujukan untuk *user* lain pada jaringan tersebut yang bertujuan untuk mendapatkan data-data penting yang ditransmisikan, biasanya disebut sebagai *Wireless Sniffing*. Salah satu cara untuk mengatasi hal ini tentunya adalah dengan mene*rap*kan enkripsi pada paket data yang ditransmisikan antara *user* dengan akses *Access Point* seperti *WEP* dan *WPA*. Namun pada kenyataannya *WEP* yang menggunakan *cipher stream RC4* dan distribusi kunci manual untuk menjaga konfidensialitas dan integritas data tidak terlalu berguna, karena *WEP* memiliki kelemahan sehingga relatif mudah untuk dibongkar [3]. Sedangkan pemakaian *WPA* relatif masih lebih aman meskipun ada beberapa fakta yang menunjukkan bahwa *WPA* dapat dibongkar dengan menggunakan metoda *brute force attack* dengan bantuan kamus *password* yang dilakukan dengan perangkat yang memiliki kemampuan komputasi tinggi.

Serangan *Man in The Middle (*MITM *)* juga dapat terjadi pada jaringan *Wifi* bahkan lebih mudah melakukannya dibandingkan pada jaringan kabel. Serangan MITM bisa terjadi karena sebelum berkomunikasi kedua pihak tidak melakukan autentikasi. Autentikasi berguna untuk memastikan identitas pihak yang berkomunikasi, apakah seseorang sedang berbicara dengan orang yang benar, atau orang ke-3 (*the person in the middle*). Gambar 2.1 menunjukkan penyerang menghubungkan perangkat *Wifi* (menggunakan wireless) ke jaringan nirkabel. Kemudian menyediakan layanan *Wifi* kepada *user* lain dengan jalur akses lain

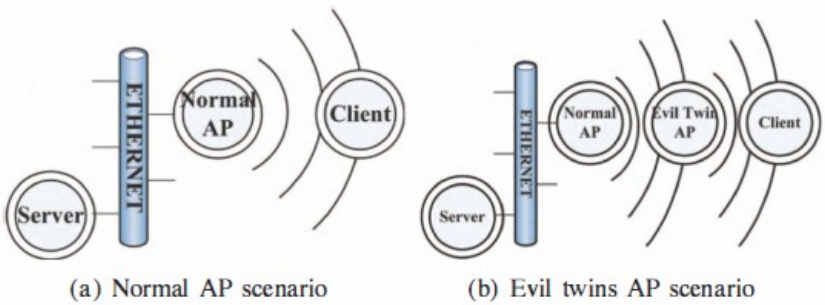
yang memiliki *SSID* yang mirip dengan *SSID* yang sesungguhnya. Trafik data dari sasaran kemudian baru dirutekan melalui router yang terhubung pada jaraingan. Penyerang tidak hanya menguping, namun sebenarnya dapat memodifikasi lalu lintas, menyisipkan virus dalam file unduhan, mengedit halaman web dan memanfaatkan kelemahan yang dikenal dalam *Script browser* untuk menyerang mesin sasaran bila mereka mengunjungi halaman web.



Gambar 2.1 Serangan MITM pada WLAN

2.2. *ROGUE ACCESS POINT*

Salah satu sarana untuk melakukan serangan MITM adalah dengan menggunakan *Rogue Access Point (*RAP*)*. RAP adalah merupakan *Access Point* yang tidak dipasang oleh administrator jaringan *Wifi* dan tidak memiliki legitimasi dari administrator, dalam istilah lain RAP juga disebut sebagai *Evil Twin Access Point* [4]. Pada Gambar 2.2 ditunjukkan perbedaan skenario akses pada jaringan wifi yang normal dengan yang terdapat perangkat RAP */ Evil twins AP*.



Gambar 2.2 Perbandingan Skenario Akses *user* ke AP dengan ke RAP

Sumber: Y. Song , C. Yang, and G. Gu., "Who Is Peeping at Your Passwords at Starbucks? - To Catch an Evil Twin Access Point"

Dalam implementasi RAP dapat dilakukan dengan menggunakan dua macam metoda yaitu menghubungkan *Access Point* langsung ke ethernet port yang ada pada infrastruktur jaringan kabel dan yang lainnya adalah dengan menghubungkan perangkat *Wireless* ke *Access Point* yang ada pada cakupannya.

Berdasarkan pada siapa yang melakukan implementasi RAP maka pada umumnya terdapat empat jenis tipe RAP sebagai berikut [5]:

1. RAP yang dibuat oleh pegawai: Pegawai dari suatu perusahaan atau instansi tertentu memasang *Access Point* pada jaringan LAN yang ada dalam kantornya tanpa ada persetujuan dari administrator jaringan dengan tujuan untuk mendapatkan kemudahan dan kenyamanan akses jaringan LAN di kantornya menggunakan *Wifi*. Dengan adanya RAP ini mengakibatnya terbukanya celah keamanan pada jaringan, yaitu dimungkinkannya *user* yang tidak berhak atau *attacker* mengakses jaringan perusahaan atau instansi tersebut. RAP jenis ini sering muncul pada perusahaan atau instansi yang kurang memperhatikan masalah keamanan jaringan dan kurangnya sosialisasi mengenai *security awareness* bagi pegawainya.
2. Eksternal RAP yang dibuat oleh penyerang: RAP dibangun diluar jaringan komputer dan tidak terhubung ke jaringan komputer suatu perusahaan atau instansi. Biasanya digunakan perangkat *Wifi* yang memiliki pancaran sinyal yang kuat yang diarahkan ke dalam area perkantoran yang menjadi sasaran dengan menggunkan SSID yang sama namanya dengan SSID yang ada dalam jaringan *Wifi* perusahaan atau instansi sasarannya. Tujuannya adalah untuk mendapatkan informasi dari pegawai dengan cara merutekan trafik melalui RAP.
3. Internal RAP yang dibuat oleh penyerang: RAP yang dibuat oleh penyerang didalam perusahaan atau instansi dan terhubung kedalam jaringan komputernya dengan tujuan untuk memperoleh *Backdoor Access* ke jaringan LAN, biasanya RAP ini tidak menyebarkan SSID agar tidak diketahui oleh orang lain. Meskipun sulit dilakukan pada saat

implementasinya namun sekali berhasil dilakukan maka dapat menyebabkan tertembusnya keamanan jaringan komputer.

4. RAP Tetangga: Merupakan RAP yang sebenarnya adalah *Access Point* yang dibuat oleh kantor yang lokasinya berdekatan dan cakupan areanya meluas sampai ke kantor lainnya. Karena tujuannya adalah untuk memberikan akses *wifi* untuk internal kantornya maka administrator jaringan dari kantor lainnya tidak berhak atau tidak memiliki akses untuk mematikannya. Meskipun tidak bertujuan jahat namun akses kedalam RAP Tetangga dapat menyebabkan celah keamanan.

2.3 PRINSIP DETEKSI *ROGUE ACCESS POINT*

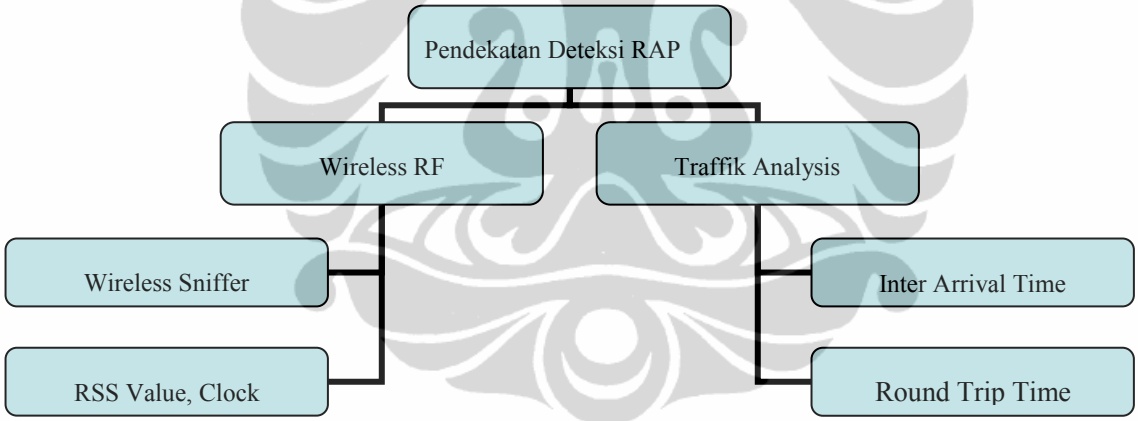
Keberadaan RAP telah menarik perhatian para peneliti ataupun vendor komersial untuk melakukan upaya pendeteksiannya. Pendekatan yang dilakukan terdiri dari dua kategori besar yaitu Pendekatan *Wireless RF* dan pendekatan Analisa Trafik seperti ditunjukkan pada Gambar 2.3.

Pendekatan *Wireless RF* menggunakan *wireless sniffer* untuk memonitor trafik *wifi* untuk kemudian dianalisis. Pada awalnya data tersebut berupa MAC *address* dari seluruh AP yang ada yang kemudian dibandingkan dengan MAC *addres list* sehingga MAC yang tidak sesuai diiindikasikan sebagai RAP. Namun setelah RAP diketahui mampu melakukan MAC *spoofing* maka jenis data yang dikumpulkan dialihkan pada data *RSS values* [6], *clock skews* [7], dan variasi frekuensi radio [8] untuk mengidentifikasi RAP.

Pendekatan yang kedua berupa analisa trafik bertujuan untuk mendeteksi apakah *user* terhubung ke jaringan melalui koneksi kabel atau nirkabel berdasarkan karakteristik paket yang ditransmisikan. Pada [1] dan [9] digunakan jarak antar paket (*Inter Arrival Time*) untuk membedakan asal paket. Standar nirkabel CSMA/CA dan properti fisik seperti kanal *duplex/ half duplex* juga membantu untuk membedakan trafik nirkabel dari trafik kabel. Analisa trafik pada gateway atau router juga dapat digunakan untuk menentukan apakah peragkat yang terhubung merupakan *user* atau sebaliknya adalah sebuah RAP.

Solusi yang ditawarkan untuk mendeteksi RAP diatas sebagian besar harus melibatkan peran serta administrator jaringan dan membutuhkan perangkat *server*

atau *appliance* yang membutuhkan investasi yang cukup mahal. Hanya ada beberapa studi yang melakukan pendekatan dari sisi *user* untuk mendeteksi adanya RAP. Salah satunya pada [2] melakukan implementasi deteksi RAP pada sisi end *user* dengan menggunakan algoritma berbasis pewaktuan yang bekerja hanya bergantung pada protokol jaringan *existing* serta dapat diaplikasikan pada jaringan Wifi tanpa campur tangan administrator. Sedangkan pada [4] juga melakukan pendekatan pada sisi end *user* untuk mendeteksi adanya RAP namun menggunakan dua macam algoritma yaitu *Trained Mean Matching (*TMM*)* dan *Hop Differentiating Technique (*HDT*)* dimana keduanya menggunakan *Sequential Probability Ratio Test (*SPRT*)*. Algoritma TMM membutuhkan *server Inter Arrival Time (server* IAT*)* sebagai penentu deteksi, sedangkan algoritma HDT tidak dan hanya ditentukan oleh analisis teoritis sehingga sesuai untuk skenario jika tidak diketahui adanya *server* IAT.



Gambar 2.3 : Pendekatan Deteksi RAP

2.4 PRINSIP DETEKSI ACCESS POINT DENGAN ALGORITMA BERBASIS PEWAKTUAN RTT

Deteksi *Rogue Access Point* dengan algoritma berbasis pewaktuan merupakan deteksi RAP dengan menggunakan pendekatan analisis trafik. RTT digunakan sebagai dasar Algoritma Berbasis Pewaktuan, hal ini dikarenakan dua hal; pertama pada saat *user* tehubung ke jaringan melalui RAP maka semua paketnya akan dilewatkan melalui dua buah hop, satu hop antara *user* dengan

RAP, satu hop lagi antara RAP dengan AP yang sesungguhnya. Hal ini berbeda jika *user* terhubung langsung dengan AP karena hanya terdapat satu hop, sehingga hop tambahan pada RAP tadi mengakibatkan bertambahnya waktu latency untuk transmisi data. Yang kedua adalah dengan perhitungan RTT maka memudahkan dalam implementasi karena tidak diperlukan peralatan khusus bagi *user* serta tidak memerlukan modifikasi pada sisi jaringan Wifi.

Namun dalam penerapan metoda berbasis RTT ini tidak bisa dilakukan secara langsung tapi harus mempertimbangkan tiga masalah berikut supaya pendeteksian RAP dapat efektif.

(1) *Server* yang akan dikontak. *Server* yang berada pada jaringan lokal lebih bagus dibandingkan menggunakan *server* yang terletak pada internet dikarenakan faktor routing dan trafik internet berpengaruh signifikan pada variasi RTT.

(2) Jenis paket apa yang akan dipakai untuk probing. Hal ini penting agar paket yang dipakai probing tidak mudah untuk dimanipulasi oleh RAP dan juga dapat menjangkau *server* yang dikontak pada berbagai setting jaringan yang berbeda-beda serta supaya tidak memerlukan bantuan network provider untuk melewatkan jenis paket yang dipakai *probing* tersebut.

(3) Yang terakhir harus dipertimbangkan kondisi trafik jaringan, dimana pada kondisi kanal yang sibuk maka akan berpengaruh pada pewaktuan RTT yang akan berakibat kesalahan pendeteksian RAP.

Dalam algoritma ini *DNS lookup* dan *DHCP Request/renew* dipakai untuk probing, karena dapat mengatasi ketiga masalah tersebut. Layanan *DNS lookup* ditangani oleh sebuah node berupa *server DNS*, biasanya jaringan komputer akan memiliki *DNS server* lokal untuk mempercepat respon dari *DNS lookup*. Ada 2 tipe *DNS lookup*, yang pertama adalah reqursive query dan kedua adalah non recursive query. *Recursive query* akan memneruskan *query* ke *DNS server* diatasnya apabila ada *query* dari *user* yang tidak dapat diresolve, sedangkan pada non reqursive query tidak dilakukan *forwarding query* dan akan memberikan pemberitahuan "*no such hostname*" sebagai respons apabila *host* yang diquery tidak ditemukan di lokal *DNS cache*. RTT dihitung berdasarkan waktu yang dibutuhkan untuk melakukan query *DNS lookup* sampai ada respon dari *DNS server* yang diterima oleh *host*.

Sedangkan *DHCP Request/renew* biasa digunakan dijaringan untuk melakukan *update* pada *IP address* yang sudah diberikan oleh *DHCP server* pada saat pertama kali *host* terhubung ke jaringan. Pada implementasi RAP umumnya RAP juga berfungsi sebagai *DHCP Server* bagi *host* yang terhubung ke jaringannya hal ini dikarenakan agar RAP dapat mengontrol IP addres yang digunakan oleh *host* agar sama dengan yang didapatkan *host* apabila terkoneksi dengan AP yang sebenarnya.

Kedua Layanan *DNS lookup* dan *DHCP Request/renew* in juga tidak memiliki masalah terkait dengan pembatasan oleh perangkat keamanan seperti firewall maupun IPS karena merupakan servise dasar yang harus dibuka pada setiap jaringan sehingga paket data dari kedua layanan tersebut dapat dikirim dan diterima oleh *host* tanpa ada paket yang terblokir.

Masalah ketiga diatasi dengan menggunakan analisa perbedaan RTT antara *DNS lookup* dan *DHCP request/renew* yang dipakai untuk menentukan pola RTT pada kedua paket tersebut pada saat kondisi trafik jaringan yang berbeda-beda. Dengan menghitung durasi waktu antara paket DNS lookup dan *DHCP Request/renew* pada kondisi trafik dan beban AP, semakin lama durasinya maka semakin sibuk kanal dari AP atau sedang melayani beban trafik yang besar.

Algoritma pendeteksian RAP berbasis Pewaktuan terbagi menjadi dua fase seperti ditunjukkan Gambar 2.4 yang berisi *pseudo code* algoritmanya. Fase pertama merupakan fase dilakukannya perhitungan RTT dan fase berikutnya adalah fase analisa RTT dan hasilnya apakah AP yang dites merupakan RAP.

Pada Fase pertama *host* melakukan *DHCP request*/*renew* dan *DNS lookup* secara berulang sejumlah n kali, kemudian RTT_{DHCP} dan RTT_{DNS} mencatat durasi RTT masing-masing. T_{data} merupakan waktu yang diperlukan untuk mentransmisikan paket *DHCP* dan *DNS* yang memiliki ukuran paket dan rate transmisi yang berbeda, sehingga dipakai untuk pengurangan RTT_{DHCP} dan RTT_{DNS}. Jumlah pengulangan n berperan dalam akurasi pendeteksian meskipun juga berakibat pada meningkatnya *overhead*.

Algorithm 1 Detecting Rogue AP (AP_x)

1: Connect and associate with AP_x
2: **for** $i = 1$ to n **do**
3: Send *unicast* probe request to AP_x, record round trip time $RTT_{probe} = RTT_{probe} - T_{data}(probe)$.
4: Send DNS lookup to local DNS server, record round trip time $RTT_{dns} = RTT_{dns} - T_{data}(dns)$.
5: **end for**
6: Filter outliers
7: $\overline{RTT_{probe}}$ = Mean of remaining RTT_{probe}
8: $\overline{RTT_{dns}}$ = Mean of remaining RTT_{dns}
9: σ_{probe} = Standard deviation of remaining RTT_{probe}
10: σ_{dns} = Standard deviation of remaining RTT_{dns}
11: $\Delta t = \overline{RTT_{dns}} - \overline{RTT_{probe}}$
12: $\theta = f(\sigma_{probe}, \sigma_{dns})$
13: **if** $\Delta t > \theta$ **then**
14: AP_x is a rogue AP
15: **end if**

Gambar 2.4: Pseudo Code Algoritma pendeteksian RAP berbasis RTT

Sumber: Hao Han, Bo Shen, Chiu C. Tan, Qun Li., Sanglu Lu., "A Measurement Based Rogue AP Detection Scheme"

Pada fase kedua dilakukan perhitungan nilai rata-rata dan standar deviasi dari RTT_{DHCP} dan RTT_{DNS}. Perbedaan nilai rata-rata RTT_{DHCP} dan RTT_{DNS} menghasilkan Δt yang akan dibandingkan dengan θ yang merupakan parameter ambang batas sebagai fungsi dari standar deviasi dari RTT_{DHCP} (σ_{DHCP}) dan RTT_{DNS} (σ_{DNS}).

Berdasarkan mekanisme standar 802.11 maka waktu pengiriman paket (T_{data}) dapat dihitung sebagai berikut:

$$T_{data}(L,r) = t_{PCLP} + \frac{(28+L).\ 8bits}{r} \quad \text{.....(2.1) [2]}$$

dimana t_{PCLP} merupakan waktu untuk transmisi paket *overhead* dari standar 802.11(dapat dilihat pada Tabel 2.1) sedangkan L dan r masing-masing adalah ukuran byte dan laju transmisi paket data.

Tabel 2.1 Karakteristik IEEE 802.11

Parameters	Values		
	802.11b	802.11g	802.11a
t_{slot}	20 μs	9 μs	9 μs
t_{DIFS}	50 μs	34 μs	28 μs
t_{PCLP}	192/96 μs	192/96 or 20 μs	20 μs
CW_{min}	31	15	15

Sumber: Hao Han, Bo Shen, Chiu C. Tan, Qun Li., Sanglu Lu., "A Measurement Based Rogue AP Detection Scheme"

Parameter ambang batas θ dapat diturunkan dengan menganalisa RTT sebagai berikut:

- Untuk AP yang sebenarnya, jalur yang dilalui *DHCP* adalah
  STA → AP → STA
  Sedangkan jalur yang dilalui *DNS lookup* dan responsnya adalah
  STA → AP → SERV → AP → STA
  Sehingga RTT_{DHCP} dan RTT_{DNS} dapat diekspresikan sebagai berikut:
  $RTT_{DHCP} \approx T_{sta \rightarrow ap} + T_{ap \rightarrow sta}$ ..... (2.2)[2]
  dan
  $RTT_{DNS} \approx T_{sta \rightarrow ap} + T_{kabel} + T_{ap \rightarrow sta}$ .....(2.3)[2]
  sehingga

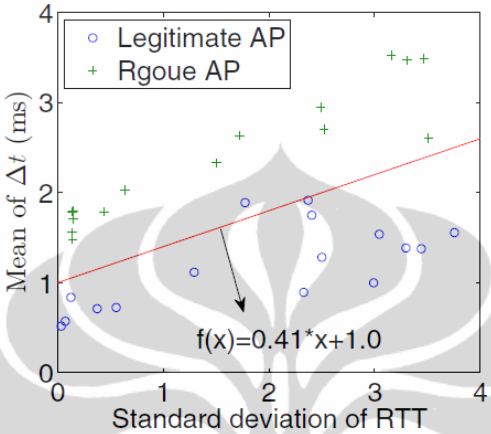
$$\Delta t = \overline{RTT_{dns}} - \overline{RTT_{dhcp}} = T_{kabel} \quad \text{.....(2.4)[2]}$$

- Sedangkan untuk RAP maka, jalur yang dilalui *DHCP* adalah
  STA → RAP → STA
  Sedangkan jalur yang dilalui *DNS lookup* dan responsnya adalah
  STA → RAP → AP → SERV → AP → RAP → STA
  mirip pada ekspresi sebelumnya diperoleh

$$\Delta t' = \overline{RTT_{dns}} - \overline{RTT_{dhcp}} = T_{rap \rightarrow ap} + T_{kabel} + T_{ap \rightarrow rap} \quad \text{.....(2.5)[2]}$$

Untuk memperoleh efektifitas dari pendeteksian maka Parameter ambang batas θ harus diantara Δt dan Δt' atau $\Delta t < \theta < \Delta t'$.

Sesuai dengan hasil eksperimen yang telah dilakukan oleh para peneliti sebelumnya [2] yang menggunakan algoritma ini diperoleh hubungan antara θ dengan standar deviasi dari RTT_{DHCP} dan RTT_{DNS} seperti ditunjukan pada Gambar 2.5.



Gambar 2.5: Hubungan antara Standar deviasi RTT dengan Rata-Rata Δt

Sumber: Hao Han, Bo Shen, Chiu C. Tan, Qun Li., Sanglu Lu., "A Measurement Based Rogue AP Detection Scheme"

Grafik diatas dapat diekspresikan dengan persamaan garis linier sebagai berikut:

$$\theta = f(\sigma_{dhcp}, \sigma_{dns}) = 0{,}41 * 0{,}5 (\sigma_{dhcp} + \sigma_{dns}) + 1 \quad \text{.....(2.6)}$$

dimana :

σ_{DHCP} adalah standar deviasi dari RTT_{DHCP}

σ_{DNS} adalah standar deviasi dari RTT_{DNS}

2.5 PERANGKAT LUNAK PENDUKUNG SISTEM DETEKSI *ROGUE ACCESS POINT*

a. Linux

Linux merupakan sistem operasi bertipe Unix modular. Linux memiliki banyak disain yang berasal dari disain dasar Unix yang dikembangkan dalam kurun waktu 1970-an hingga 1980-an. Linux menggunakan sebuah kernel monolitik, kernel Linux yang menangani kontrol proses, jaringan, periferal dan pengaksesan sistem berkas. *Device driver* telah terintegrasi ke dalam

kernel. Banyak fungsi-fungsi tingkat tinggi di Linux ditangani oleh proyek-proyek terpisah yang berintegrasi dengan kernel. Userland GNU merupakan sebuah bagian penting dari sistem Linux yang menyediakan shell dan peralatan-peralatan yang menangani banyak fungsi-fungsi dasar sistem operasi. Di atas kernel, peralatan-peralatan ini membentuk sebuah sistem Linux lengkap dengan sebuah antarmuka pengguna grafis yang dapat digunakan, umumnya berjalan di atas X *Window System*.

b. Apache Web*server*

Apache Web*server* adalah *server* web yang dapat dijalankan di banyak sistem operasi (Unix, BSD, Linux, Microsoft Windows dan Novell Netware serta *platform* lainnya) yang berguna untuk melayani dan memfungsikan situs web. Protokol yang digunakan untuk melayani fasilitas web/www ini menggunakan HTTP atau HTTPS. Apache memiliki fitur-fitur canggih seperti pesan kesalahan yang dapat dikonfigurasi, autentikasi berbasis *Database* dan lain-lain. Apache juga didukung oleh sejumlah antarmuka pengguna berbasis grafik (GUI) yang memungkinkan penanganan *server* menjadi mudah. Apache merupakan perangkat lunak sumber terbuka dikembangkan oleh komunitas terbuka yang terdiri dari pengembang-pengembang dibawah naungan Apache Software Foundation.

Sistem yang dikembangkan penulis memanfaatkan Apache untuk menangani request dari *user* yang akan melakukan pendeteksian RAP terhadap *Access Point* yang digunakannya melalui halaman web yang tersedia sebagai antarmuka sistem. Setelah aplikasi deteksi RAP menghasilkan analisa mengenai *Access Point* yang diuji dan sudah ada hasilnya baru ditampilkan di halaman web oleh Apache.

c. Database MySQL

MySQL adalah sebuah implementasi dari sistem manajemen basisdata relasional (RDBMS) yang didistribusikan secara gratis dibawah lisensi *General Public License* (GPL). Setiap pengguna dapat secara bebas menggunakan MySQL, namun dengan batasan perangkat lunak tersebut tidak boleh dijadikan produk turunan yang bersifat komersial. MySQL sebenarnya merupakan turunan salah satu konsep utama dalam basisdata yang telah ada

sebelumnya; *Structured Query Language* (SQL). SQL adalah sebuah konsep pengoperasian basisdata, terutama untuk pemilihan atau seleksi dan pemasukan data, yang memungkinkan pengoperasian data dikerjakan dengan mudah secara otomatis.

Kehandalan suatu sistem basis data (DBMS) dapat diketahui dari cara kerja optimasinya dalam melakukan proses perintah-perintah SQL yang dibuat oleh pengguna maupun program-program aplikasi yang memanfaatkannya. Sebagai pelayan basis data, MySQL mendukung operasi basisdata transaksional maupun operasi basisdata non-transaksional. Pada modus operasi non-transaksional, MySQL dapat dikatakan unggul dalam hal unjuk kerja dibandingkan perangkat lunak pelayan basisdata kompetitor lainnya. Namun demikian pada modus non-transaksional tidak ada jaminan atas reliabilitas terhadap data yang tersimpan, karenanya modus non-transaksional hanya cocok untuk jenis aplikasi yang tidak membutuhkan reliabilitas data seperti aplikasi blogging berbasis web, CMS, dan sejenisnya. Untuk kebutuhan sistem yang ditujukan untuk bisnis sangat disarankan untuk menggunakan modus basisdata transaksional, hanya saja sebagai konsekuensinya unjuk kerja MySQL pada modus transaksional tidak secepat unjuk kerja pada modus non-transaksional.

Alasan menggunakan MySQL sebagai pelayan basisdata adalah karena MySQL memiliki berbagai keunggulan sebagai berikut:

- Portabilitas. MySQL dapat berjalan stabil pada berbagai sistem operasi seperti Windows, Linux, FreeBSD, Mac Os X *Server*, Solaris, Amiga, dan masih banyak lagi.
- Perangkat lunak sumber terbuka. MySQL didistribusikan sebagai perangkat lunak sumber terbuka, dibawah lisensi GPL sehingga dapat digunakan secara gratis.
- *'Performance tuning'*, MySQL memiliki kecepatan yang menakjubkan dalam menangani query sederhana, dengan kata lain dapat memproses lebih banyak SQL per satuan waktu.
- Ragam tipe data. MySQL memiliki ragam tipe data yang sangat kaya, seperti *signed / unsigned integer, float, double, char, text, date*,

timestamp, dan lain-lain.

- Keamanan. MySQL memiliki beberapa lapisan keamanan seperti level *subnetmask*, nama *host*, dan izin akses *user* dengan sistem perizinan yang mendetail serta sandi terenkripsi.
- Skalabilitas dan Pembatasan. MySQL mampu menangani basis data dalam skala besar, dengan jumlah rekaman (records) lebih dari 50 juta dan 60 ribu tabel serta 5 milyar baris. Selain itu batas indeks yang dapat ditampung mencapai 32 indeks pada tiap tabelnya.
- Antar Muka. MySQL memiliki antar muka (interface) terhadap berbagai aplikasi dan bahasa pemrograman dengan menggunakan fungsi API (Application Programming Interface).
- Klien dan Peralatan. MySQL dilengkapi dengan berbagai peralatan (tool)yang dapat digunakan untuk administrasi basis data, dan pada setiap peralatan yang ada disertakan petunjuk online.

BAB 3
PERANCANGAN SISTEM DETEKSI *ROGUE ACCESS POINT* BERBASIS WEB

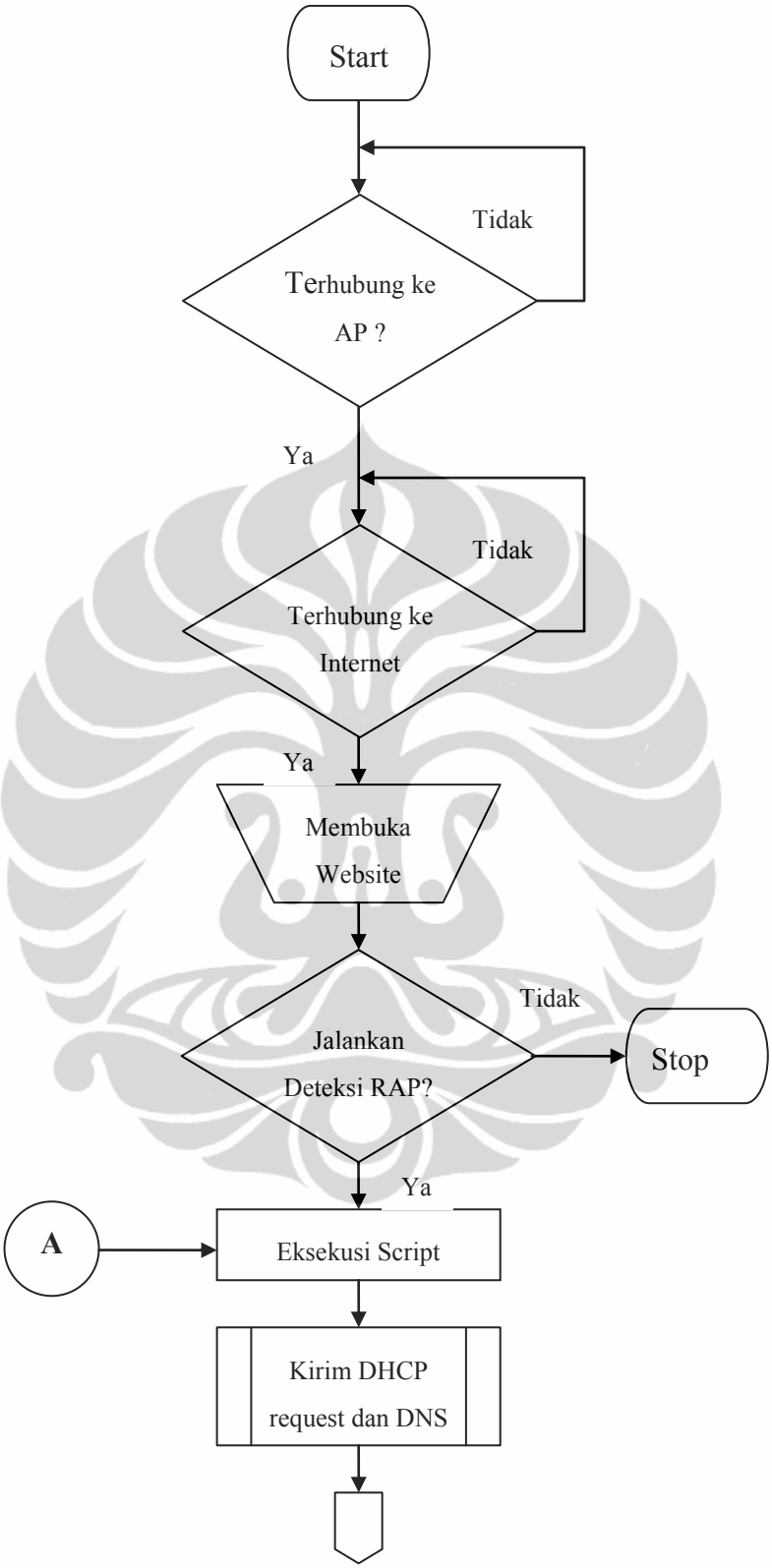
3.1. PROSES DETEKSI *ROGUE ACCESS POINT* DENGAN METODA PENGUKURAN WAKTU RTT

Untuk mendeteksi apakah *Access Point* yang digunakan oleh *user* merupakan RAP atau tidak maka *user* hanya membutuhkan web *browser* sebagai interfacenya. Hal ini tentunya sangat praktis dan mudah dibandingkan dengan yang sudah ada selama ini dimana *user* harus menginstal Perangkat Lunak tertentu atau menggunakan tools-tools yang didesain khusus untuk mendeteksi keberadaaan RAP. Proses pendeteksian RAP dimulai pada saat *user* memperoleh akses internet dari *Access Point* tertentu, kemudian *user* membuka web *browser* untuk mengakses *website* yang telah dibuat oleh penulis untuk layanan deteksi RAP secara online.

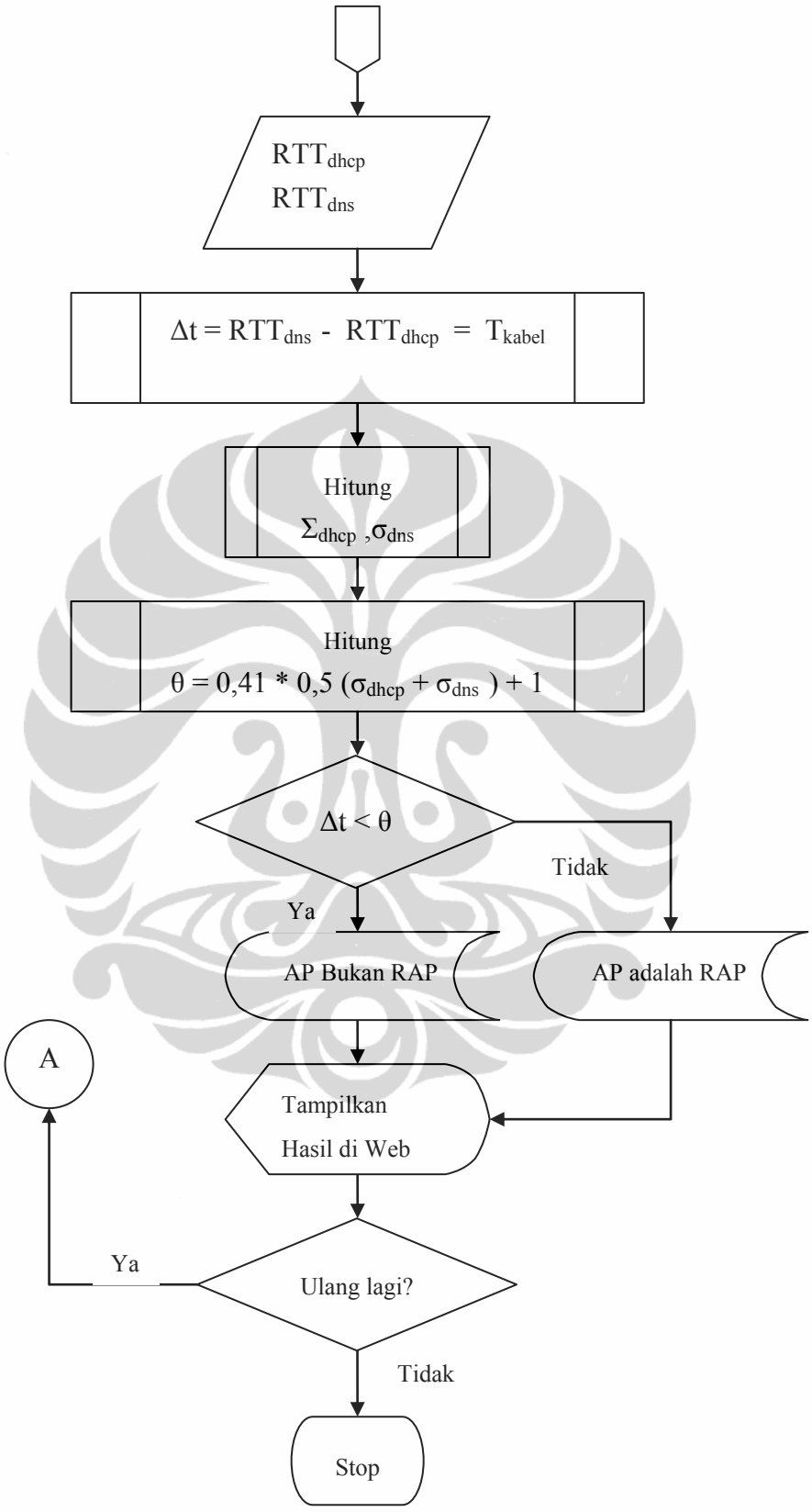
Setelah terhubung ke *website* tersebut maka *user* akan memilih menu (mengklik) icon yang disediakan untuk melakukan testing RAP. Pada saat *user* mengklik icon tersebut maka terjadi proses request terhadap aplikasi deteksi RAP yang ada di *server* yang kemudian akan memberikan respon untuk mengirimkan *Script* kepada komputer *user* dan kemudian dieksekusi. Aliran proses interaksi user dengan interface web ini ditunjukkan pada Gambar 3.1.

Script memiliki dua tugas, yang pertama menjalankan perintah pada komputer *user* untuk mengirimkan *DHCP request/renew* kepada *Access Point* yang digunakan dan mengirimkan *DNS lookup* ke *Server DNS* yang digunakan oleh komputer *user* tersebut, proses ini diulang sampai jumlah tertentu sesuai tingkat akurasi pendeteksian yang diinginkan. Tugas kedua adalah mencatat waktu dari durasi proses *DHCP request/renew* serta proses *DNS lookup* yang kemudian akan dikirimkan ke aplikasi deteksi RAP yang ada pada *server*. Proses selanjutnya terjadi di sisi *server*, dimana catatan hasil *DHCP request/renew* dan *DNS lookup* yang diterima disimpan dalam tabel yang ada dalam database aplikasi kemudian baru dilakukan perhitungan terhadap data-data tersebut untuk

mendeteksi RAP menggunakan algoritma berbasis pewaktuan. Setelah analisa selesai maka hasilnya yang menunjukkan apakah AP yang dipakai *user* merupakan RAP atau tidak dikirim ke *user* melalui web, sampai titik ini proses pendeteksian RAP selesai.



Gambar 3.1 Diagram Alir Deteksi RAP berbasis Pengukuran waktu RTT



Gambar 3.1 Diagram Alir Deteksi RAP berbasis Pengukuran waktu RTT "Sambungan"

3.2. PROSES PENGOLAHAN DATA PENGUKURAN WAKTU *RTT* DI *SERVER*

Data RTT_{DHCP} dan RTT_{DNS} yang dikirim ke Web*server* kemudian diolah oleh aplikasi deteksi RAP yang sudah di install di *server*. Setelah itu data tersebut disimpan terlebih dahulu kedalam tabel *Data DHCP* dan *DNS* yang ada dalam database. Algoritma yang dipakai adalah Algoritma Pengukuran Waktu RTT yang sudah dijelaskan pada bagian sebelumnya. Hasil pengolahan data akan menghasilkan parameter yang akan dipakai untuk menentukan apakah *Access Point* yang diuji merupakan RAP atau tidak. Parameter-parameter tersebut adalah:

- Δt merupakan waktu transmisi paket pada kabel

$$\Delta t = \overline{RTT_{dns}} - \overline{RTT_{dhcp}} = T_{kabel} \quad \text{..... (3.1)}$$

- $\Delta t'$ merupakan waktu transmisi paket pada kabel dan antara *AP* dengan RAP

$$\Delta t' = \overline{RTT_{dns}} - \overline{RTT_{dhcp}} = T_{rap \rightarrow ap} + T_{kabel} + T_{ap \rightarrow rap} \quad \text{.....(3.2)}$$

- Parameter ambang batas θ

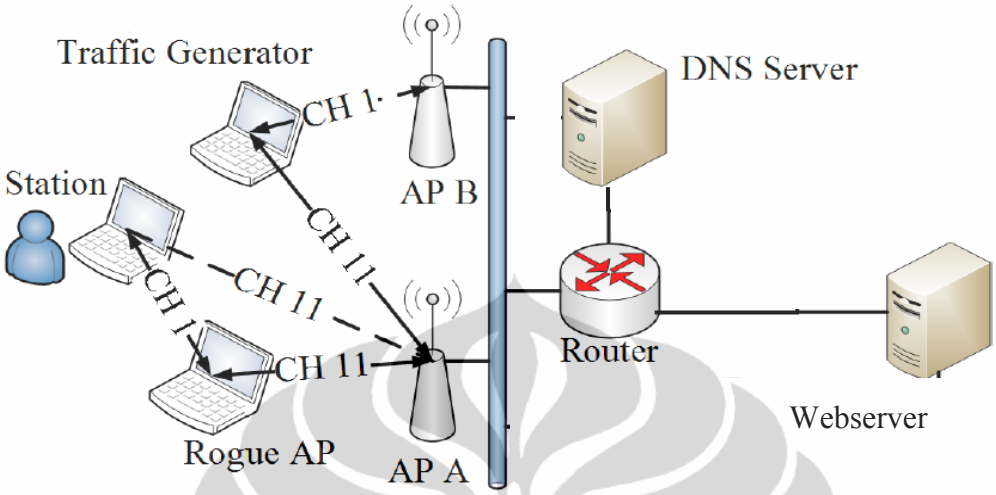
$$\theta = f(\sigma_{dhcp}, \sigma_{dns}) = 0{,}41 * 0{,}5 (\sigma_{dhcp} + \sigma_{dns}) + 1 \quad \text{.....(3.3)}$$

Setelah ketiga parameter diatas diperoleh maka aplikasi baru dapat menentukan apakah *Access Point* yang diuji merupakan RAP atau tidak dengan kriteria jika Δt lebih besar daripada θ maka *Access Point* tersebut adalah RAP tapi jika sebaliknya maka *Access Point* tersebut adalah *Access Point* yang sebenarnya.

3.3. TOPOLOGI JARINGAN

Perancangan deteksi *rogue access point* yang diusulkan akan diimplementasikan pada topologi jaringan seperti diperlihatkan pada Gambar 3.2. Skenario pada gambar tersebut menunjukkan bahwa ada *user* yang terhubung ke *Access Point* dan ada juga yang terhubung ke RAP. User dapat mengakses Web*server* melalui dua buah jalur, pertama melalui *Access Point* yang terhubung ke router mengunakan jaringan kabel; kedua melalui RAP terlebih dahulu

sebelum melalui *Access Point* ke router. *DNS Server* terletak pada jaringan lokal yang terhubung dengan *Access Point* menggunakan infrastruktur kabel.



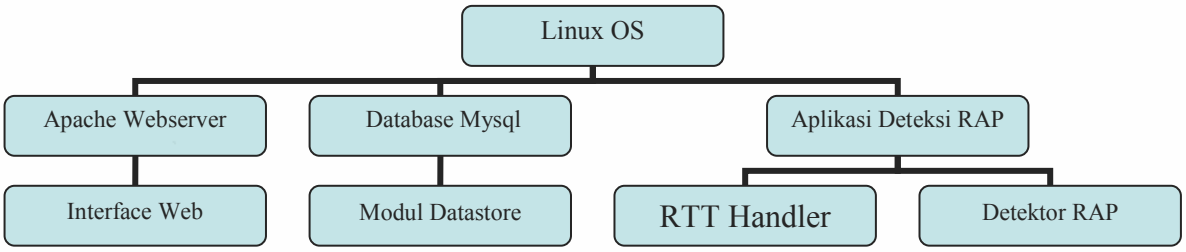
Gambar 3.2. Topologi Skenario Deteksi RAP

Sumber: Hao Han, Bo Shen, Chiu C. Tan, Qun Li., Sanglu Lu., "A Measurement Based Rogue AP Detection Scheme" (telah diolah kembali)

Pada Skenario diatas juga digunakan sebuah *Station* yang berfungsi sebagai Traffic Generator yang digunakan untuk mewakili kondisi jaringan Wireless LAN yang sedang diakses oleh *user*.

3.4. PERANGKAT LUNAK DAN PERANGKAT KERAS PENDUKUNG SISTEM

Untuk melayani *user* yang ingin mendeteksi *Access Point* yang sedang dipakai apakah merupakan RAP atau tidak maka dibuat *website* yang diletakkan pada web*server*. Web*server* akan diinstal pada *Server* dengan OS linux distro Ubuntu dengan menggunakan Web*legitimate* *AP*ache versi 2.2.14. Untuk menyimpan data hasil pendeteksian RAP digunakan Database MySQL versi 5.1.41. Struktur perangkat lunak yang digunakan dalam sistem ini ditunjukkan dalam Gambar 3.3.



Gambar 3.3. Struktur Perangkat Lunak *Server*

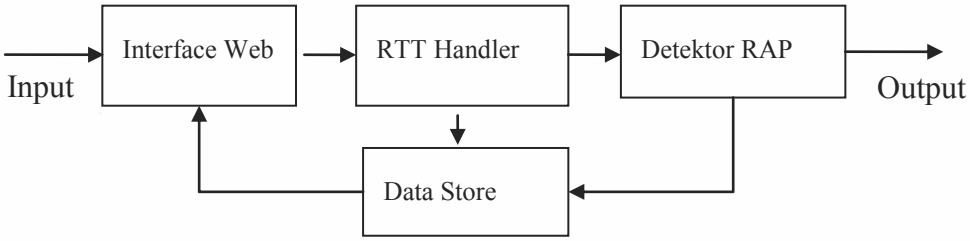
Dalam implementasinya direncanakan akan digunakan perangkat lunak dan keras sebagai berikut:

a) Perngkat Lunak:
   1) *Apache Webserver*
   2) *MySQL Database*
   3) *Linux Ubuntu*
   4) *Client Side Script*

b) Perangkat Keras:
   1) *Access Points:* Menggunakan sebuah *Access Point* Linksys WPA54G yang akan dioperasikan pada 802.11b/g.
   2) *Wireless Stations*: Digunakan laptop dengan processor intel dengan kecepatan minimal setara Centrino yang masing-masing menggunakan *WLAN card* internal. Khusus untuk laptop yang digunakan sebagai RAP dilengkapi dengan *WLAN card* eksternal.
   3) *DNS server*: Sebagai DNS *server* akan digunakan komputer Desktop yang terhubung ke jaringan dengan menggunakan *ethernet*.
   4) *Web Server*: Akan digunakan komputer Desktop yang terhubung ke jaringan dengan menggunakan *ethernet*.

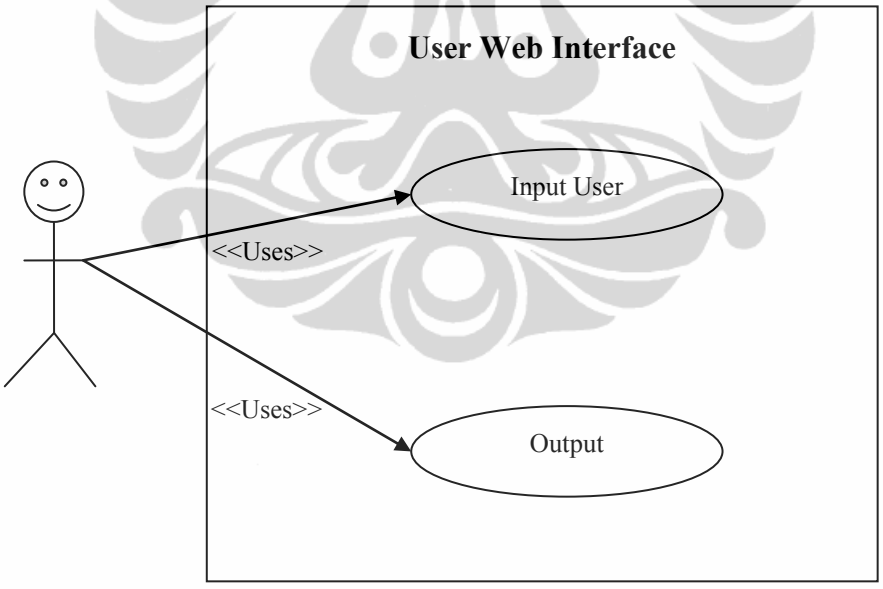
3.5 APLIKASI DETEKTOR RAP

Aplikasi Detektor RAP yang dikembangkan dalam sistem ini memiliki Blok Diagram seperti yang ditunjukkan pada Gambar 3.4.



Gambar 3.4 Blok Diagram Aplikasi Detektor RAP

Aplikasi Detektor RAP merupakan inti dari Sistem Pendeteksi Rogue Access Point. Aplikasi inilah yang akan mengolah data yang diperoleh dari hasil *DHCP* dan *DNS lookup* dari komputer *user*, kemudian menganalisanya dengan menggunakan algoritma yang sudah ditentukan untuk menentukan apakah Access Point yang digunakan *user* merupakan *Rogue Access Point* atau tidak. Selanjutnya menampilkan hasil analisanya kepada *user* melalui interface web.



Gambar 3.5 Use Case Diagram dari Modul *Web Interface*

Aplikasi Deteksi RAP terdiri dari beberapa modul yang memiliki fungsi berbeda-beda sesuai dengan perannya masing-masing. Modul-modul tersebut adalah Modul Interface Web, Modul Database, dan Modul Detektor RAP.

- Modul *Web Interface*: Sistem berinteraksi dengan *user* menggunakan web

sebagai *Graphical User Interface (GUI)*. Modul ini bertugas untuk mengambil input dari *user* serta menampilkan output ke *user*. Interaksi *user* dengan sistem melalui Modul Interface ditunjukkan pada Gambar 3.5 sebelumnya.

- Modul RTT Handler: Modul ini bertugas untuk menerima dan mencatat data RTT_{DHCP} dan RTT_{DNS} yang dikirimkan oleh komputer *user* melalui interface web. Data ini disimpan sementara dalam buffer data untuk kemudian diolah untuk memperoleh data statistik, baru data statistik tersebut diteruskan ke Modul Detektor RAP untuk dianalisa menggunakan Algoritma Pengukuran Waktu RTT. Data statistik yang diolah oleh modul *RTT Handler* tampak pada Tabel 3.1.

Tabel 3.1 : Data Statistik pada Modul Data Handler

NO	Input	Output
1	RTT_{DHCP}	$\overline{RTT_{DHCP}}$ dan σ_{DHCP}
2	RTT_{DNS}	$\overline{RTT_{DNS}}$ dan σ_{DNS}

- Modul Detektor RAP

  Data keluaran dari Modul RTT yang sudah berupa data statistik dari RTT_{DHCP} dan RTT_{DNS} menjadi bahan untuk dianalisa oleh modul ini untuk ditentukan hasil analisanya apakah Access Point yang dipakai merupakan RAP atau tidak. Analisa pendeteksian RAP dilakukan sesuai pseudo code berikut ini:

Pseudo Code untuk Deteksi RAP

1: $\Delta t = \overline{RTT_{DNS}} - \overline{RTT_{DHCP}}$

2: $\theta = f(\sigma DHCP, \sigma DNS)$

3: if $\Delta t > \theta$ then

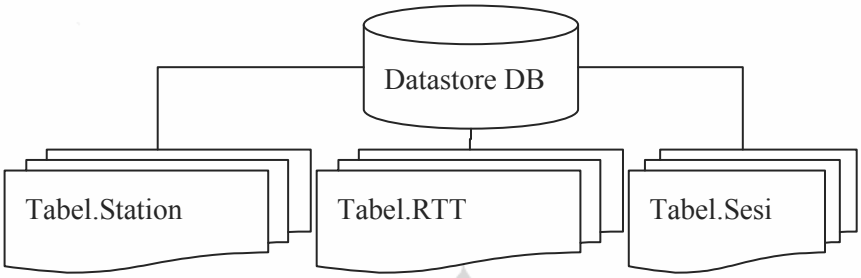
4: APx is a rogue AP

5: end if

- Modul Data Store

  Modul Data Store bertugas menyimpan data yang diinputkan oleh *user* melalui interface Web dan juga data hasil olahan modul Modul RTT Handler serta Modul Detektor RAP untuk digunakan lagi apabila diperlukan oleh sistem. Modul ini menggunakan MySQL sebagai manajemen system dari

databasenya. Database yang ditangani oleh modul ini terdiri dari beberapa tabel yang menyimpan data input dan output dari sistem deteksi RAP ini.



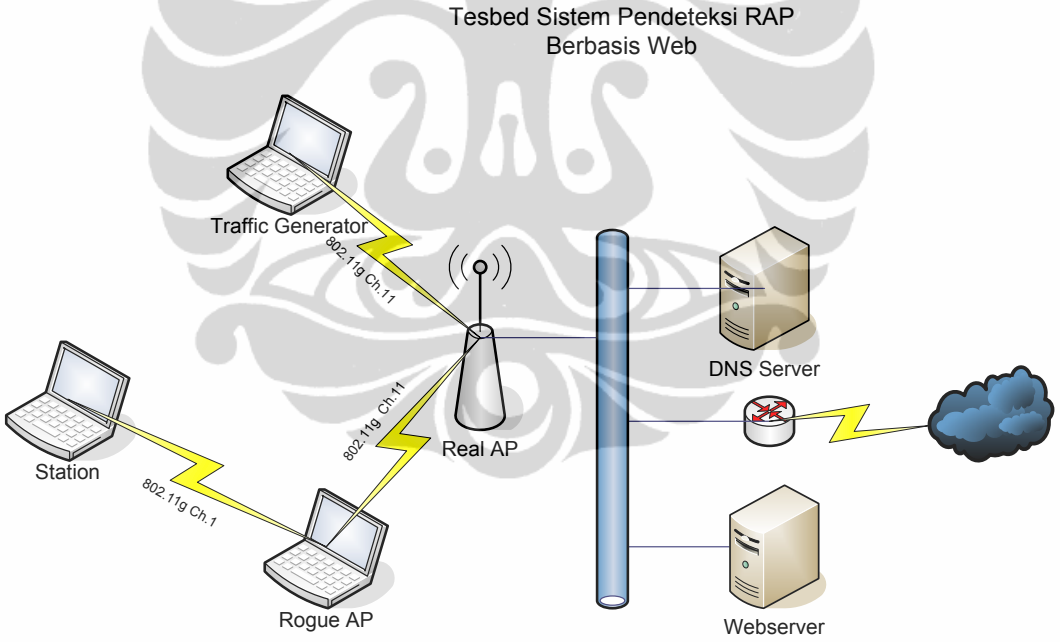
Gambar 3.6 Tabel Database Modul Datastore

BAB 4
IMPLEMENTASI DAN PENGUJIAN

4.1 Setup dan Implementasi *Testbed*

Setup dan implementasi *Testbed* yang menggambarkan kondisi jaringan komputer terlebih dulu dilakukan sebelum dilakukan tahap pengujian terhadap Sistem Pendeteksi RAP Berbasis Web dengan berbagai skenario yang ada.

Pada implementasi Testbed ini ada tiga jaringan yang saling terhubung satu dengan lainnya yaitu (1)Wireless Network antara Station, RAP dan *Legitimate AP* , (2)LAN yang menghubungkan Legitimated AP dengan Server DNS dan Server Web, dan (3) Internet. Topologi Jaringan Testbed Dapat dilihat pada Gambar 4.1.



Gambar 4.1 Topologi *Testbed* Sistem Pendeteksi RAP Berbasis Web

Testbed ini diimplementasikan pada ”Computer HomeLab” yang dimiliki oleh penulis yang merupakan interkoneksi dari beberapa *host* komputer/Notebook yang sudah diinstal dengan aplikasi yang sesuai dengan perannya masing-masing didalam *Testbed* sistem pendeteksi RAP berbasis Web ini.

4.1.1 *Wireless Network*

Wireless Network terbagi menjadi 2 yaitu Jaringan WiFi yg menghubungkan antara *Station* dengan RAP dan Jaringan WiFi yang menghubungkan RAP dan Genator Trafik dengan *Legitimate AP*. Pada Jaringan WiFi yang menghubungkan *Station* dengan RAP digunakan standar 802.11g karena pada umumnya RAP akan berusaha untuk memberikan bandwidth akses yang maksimal bagi *Station* yang menjadi korbannya sehingga dengan menggunakan standar 802.11g diharapkan akan mencapai maksimal 54 Mbps. Sedangkan pada jaringan WiFi yang menghubungkan RAP dengan *Legitimate AP* menggunakan Standar 802.11b/g dengan alasan bahwa pembuat RAP tidak dapat mengontrol *legitimate* AP yang akan dijadikan gateway baginya karena RAP sebenarnya hanya menjadi klien dari *Legitimate AP* sehingga mau tidak mau harus mengikuti Standar yang digunakan oleh *Legitimate AP* tersebut. *Legitimate* AP di Testbed ini menggunakan hardware Linksys Wireless-G Broadband Router WRT54TGL seperti terlihat pada Gambar 4.2.

Gambar 4.2. Access Point Linksys WRT54GL

Dalam implementasinya kedua jaringan menggunakan kanal frekuensi radio yang berbeda, supaya tidak ada interferensi dari masing-masing jaringan. Jaringan

WiFi yg menghubungkan antara *Station* dengan RAP (menggunakan 802.11g channel 1) dan Jaringan WiFi yang menghubungkan RAP dan Genator Trafik dengan Legtimate AP (menggunakan 802.11b/g channel 11).

4.1.2 LAN menggunakan Fast Ethernet 100Mbps.

Testbed ini menggunakan jaringan LAN untuk menghubungkan antara *Legitimate AP* dengan *Server* DNS dan Web*server*. Standard yang digunakan adalah Fast Ethernet dengan bandwith maksimum 100Mbps. LAN ini kemudian terhubung dengan internet dengan menggunakan sebuah router.

4.1.3 Internet akses.

Jaringan yang ada dapat terhubung ke internet menggunakan gateway berupa Wireless 3G Modem. Akses ke internet ini dibutuhkan oleh DNS *server* untuk melakukan DNS forwarder apabila *Server* DNS mendapatkan query DNS lookup yang baru yang belum tersimpan pada Databasenya. Pemilihan Wireless 3G Modem semata-mata hanya karena alasan fleksibilitas dan kemudahannya dalam pemasangan koneksi internet, hal ini tentunya juga sudah dipertimbangkan karena penggunaan akses internet tersebut tidak akan mempengaruhi proses pengujian Aplikasi Pendeteksi RAP berbasis Web ini dikarenakan parameter-parameter yang diukur tidak ada yang terkait dengan interkoneksi dengan internet.

4.1.4 Komputer *Host*

Pada *Testbed* ini terdapat beberapa komputer *Host* yang terhubung satu dengan yang lain, diantarnya adalah *Station*, RAP, Traffic Generator, DNS *server* dan Web*server*.

4.1.4.1 *Station*

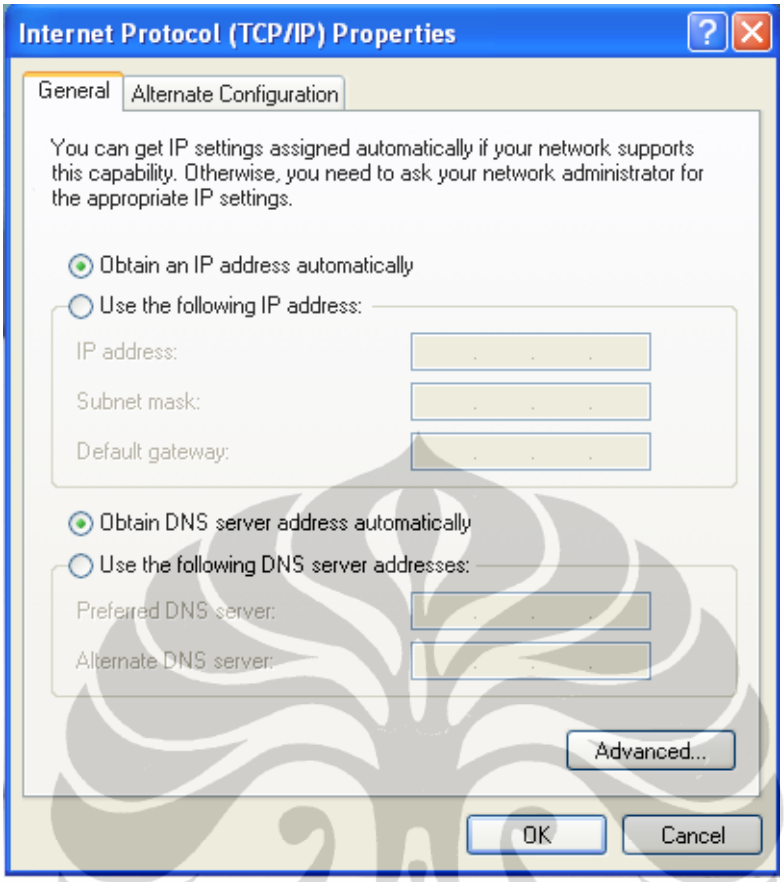
Pada implementasinya digunakan Notebook dengan OS windows XP service pack 3 sebagai *Station*. *Station* ini berfungsi sebagai *host* yang akan melakukan pendeteksian RAP mengunakan Aplikasi berbasis Web pada saat terhubung ke AP tertentu. *Station* ini terkoneksi ke jaringan WiFi dengan menggunakan interface wireless Card onboard (intel pro/wireless 3495) Wifi 802.11b/g pada channel 1

(saat terhubung dengan RAP) dan pada channel 11 (saat terhubung dengan *Legitimate AP*). Pada pengujian sistem, *Station* akan terhubung ke *Legitimate AP* atau ke RAP dan kemudian membuka *website* yang ada aplikasi pendeteksi RAP menggunakan *browser* Internet Explorer, kemudian baru dilakukan eksekusi untuk mendeteksi RAP.

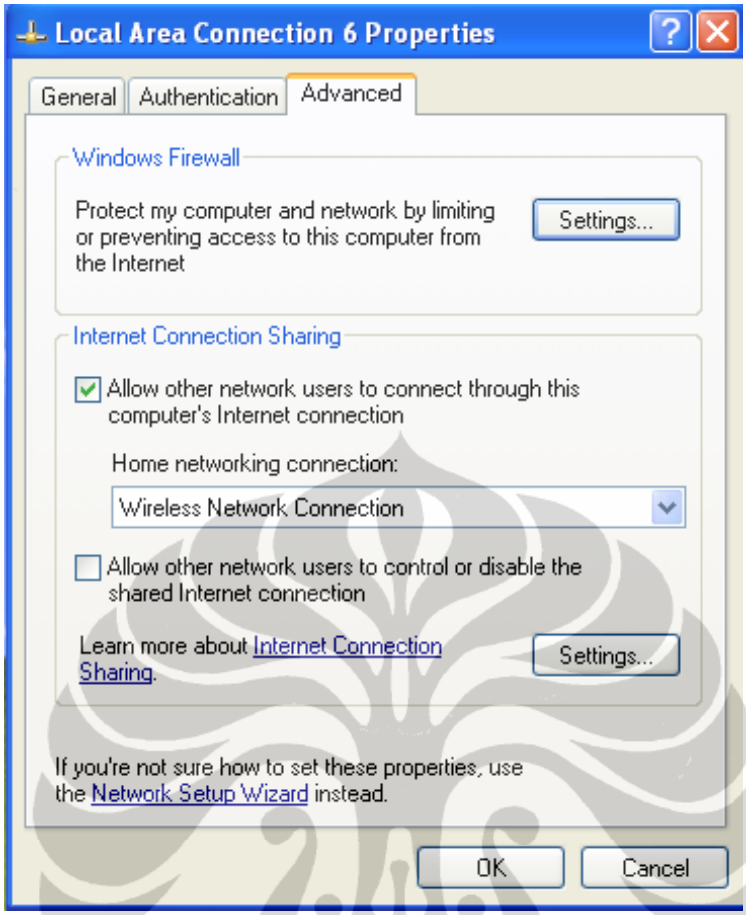
4.1.4.2 Rogue Access Point

RAP diimplementasikan dengan menggunakan Notebook (Intel Centrino 1.73 GHz RAM 1 GB) dengan OS windows XP SP 3 dengan menggunakan 1 buah kartu wireless internal (intel pro/wireless 3495) yang berfungi untuk akses koneksi ke *Legitimate AP* dan 1 buah kartu wireless eksternal (realtek 8187) yang berfungsi sebagai Rogue AP untuk *Station*. Untuk menjadikan Notebook sebagai RAP maka diperlukan konfigurasi sebagai berikut:

- Setting network properties pada kartu wireless internal diset agar TCP/IP protokol mendapat IP Dinamis dan DNS *Server* dari DHCP *server*, seperti terlihat pada Gambar 4.3. Kemudian pada Gambar 4.4 terlihat Feature Internet Connection Sharing dienable supaya user yang terkoneksi ke RAP dapat mengakses internet.

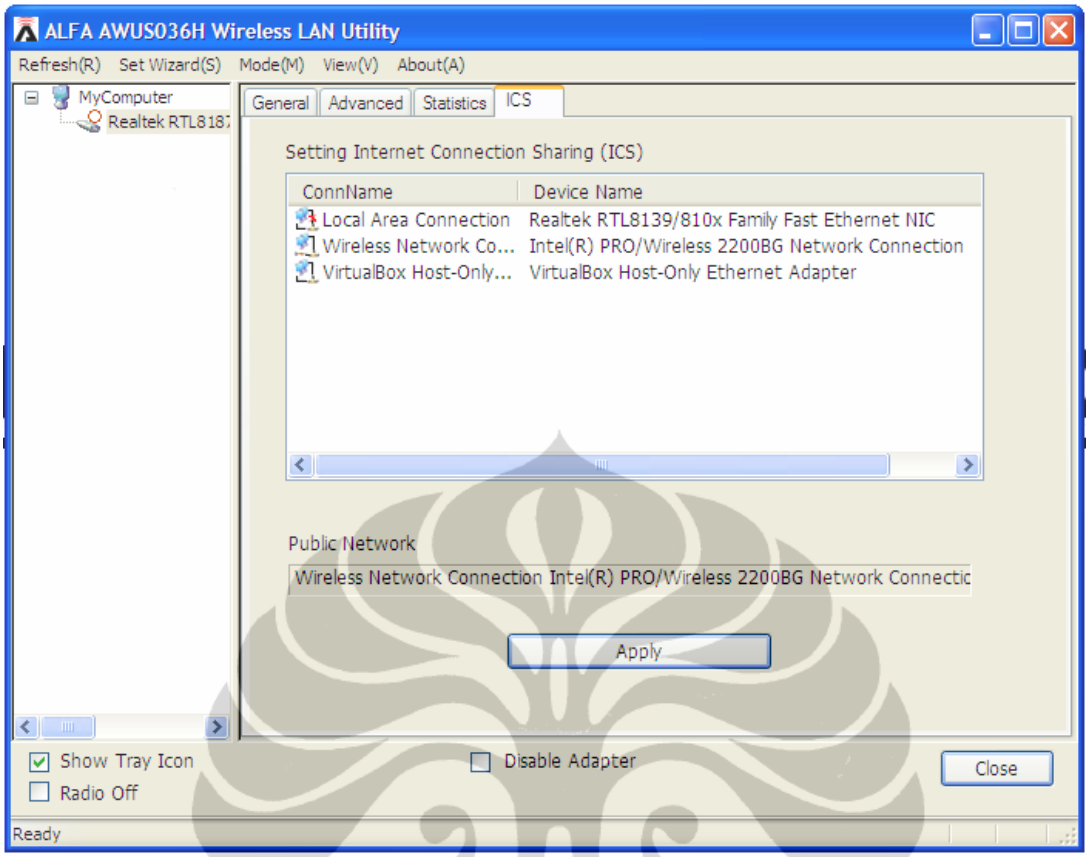


Gambar 4.3. Setting TCP/IP protokol pada RAP



Gambar 4.4. Setting Internet Connection Sharing pada RAP

- Setting pada kartu wireless eksternal dilakukan dengan menggunakan aplikasi proprietary dari vendor untuk menjadikannya sebagai Software AP yang berfungsi sebagai RAP. Dalam pengujian Soft AP ini menggunakan Setting Open *Security*. Hal ini ditunjukkan pada Gambar 4.5.



Gambar 4.5 Setting Software AP pada RAP

4.1.4.3 Server DNS

Servis DNS yang akan digunakan oleh *Station* diaplikasikan menggunakan Desktop Computer (intel core 2 duo 2.2 GHz RAM 1GB)yang dijadikan *server* DNS menggunakan OS linux 2.6 (Debian) yang dijalankan secara virtual dengan VMWare. Servis DNS dijalankan dengan menginstal servis BIND (*Berkeley Internet Name Domain*) di OS Debian tersebut. Instalasi paket bind *server*, sesuaikan dengan distro yang dipakai. Bisa dari paket melalui yum, apt-get, pkg-get, smart ato pacman, bisa juga melalui source.

Konfigurasi agar servis BIND dapat digunakan pada *Testbed* dilakukan dengan melakukan setting beberapa file yang berkaitan dengan BIND yaitu:

- Named.config

  File ini berisi konfigurasi address mana saja yang boleh melakukukan request DNS serta *Server* DNS yang akan dijadikan sebagai forwarder.

```
acl drop {
    224.0.0.0/24;
    };
acl trusted {
    localnets;
    192.168.2.0/27;
    192.168.3.28/30;
    };
acl secondaries {
    local*host*;
    };
forwarders {
            202.134.1.10;
            202.134.0.155;
            8.8.8.8;
                };
    forward only;
```

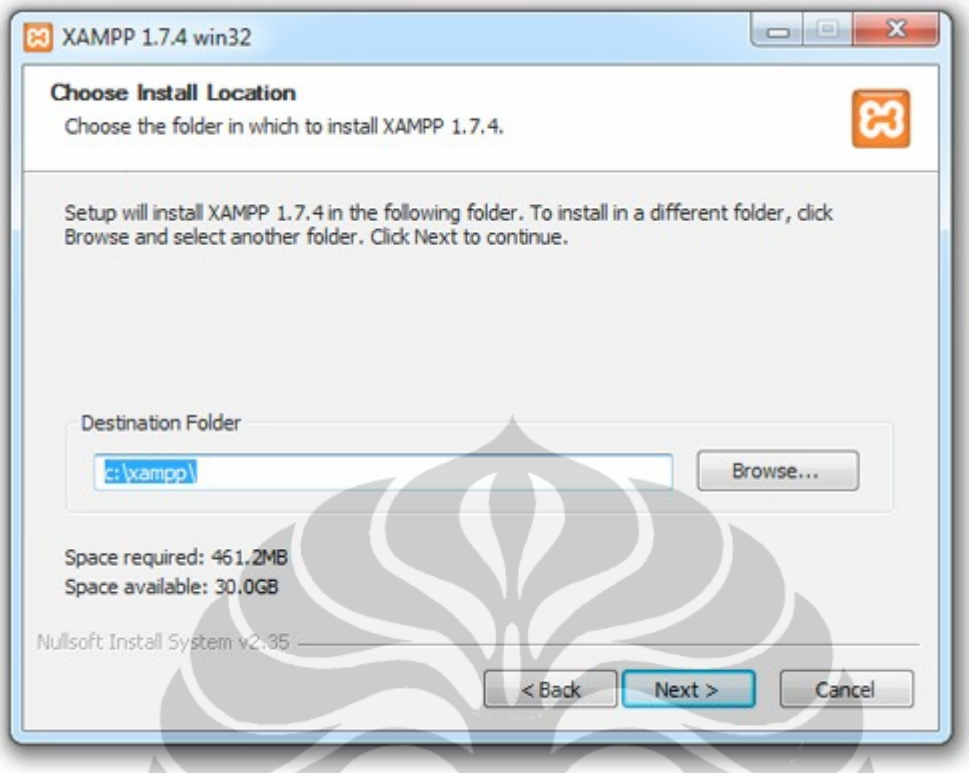
- **/etc/resolv.conf**

  File ini berfungsi agar semua request DNS ditangani oleh *server* DNS pada local*host*.

```
name*server* 127.0.0.1
name*server* 192.168.3.29
```

4.1.4.4 Server Web

Servis web dijalankan pada komputer Desktop dengan spesifikasi perangkat keras komputer adalah intel core 2 duo 2.2 GHz RAM 1GB yang dijadikan *server* DNS menggunakan OS Windows 7. Web servis yang diinstal menggunakan Xampp versi 1.7.4 yang sudah berisi dengan modul Apache web*server*, PHP , dan Database MySql. Semua servis ini diinstal pada root folder: C:/XAMPP pada saat instalasi awal seperti ditunjukkan pada Gambar 4.6 berikut ini.



Gambar 4.6 Lokasi Instalasi XAMPP

Konfiigurasi Xampp dilakukan dengan melakukan perubahan-perubahan pada 3 komponen Xampp yang sering digunakan yaitu:

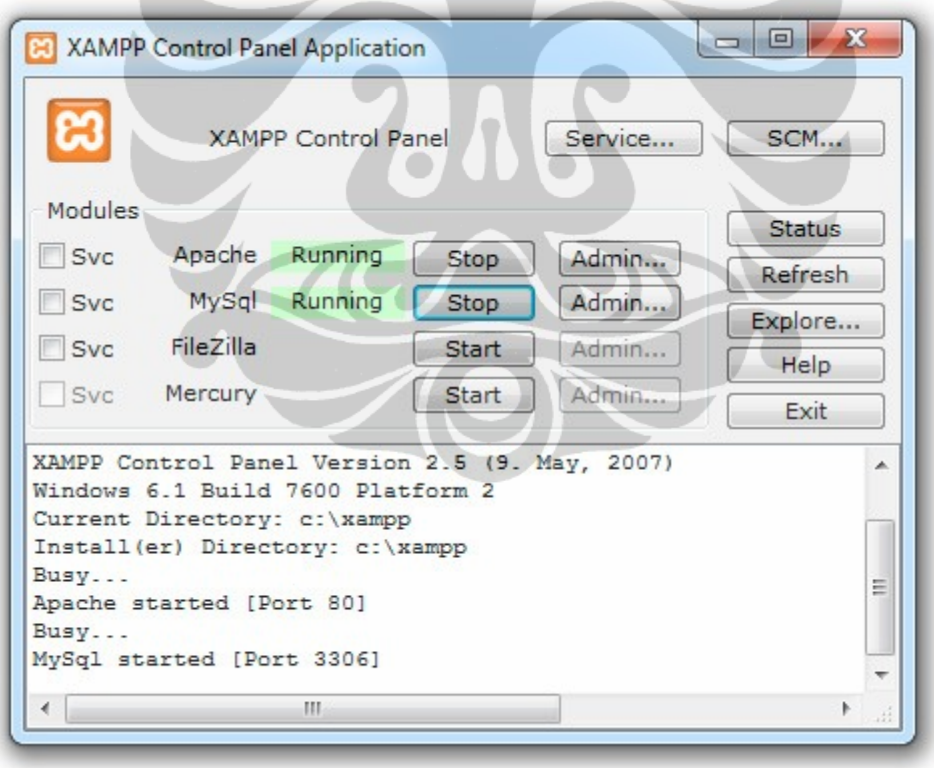
- **htdoc** adalah folder tempat meletakkan berkas-berkas yang akan dijalankan, seperti berkas PHP, HTML dan skrip lain. Htdoc ini diinstal di root folder C:/XAMPP/htdocs
- **phpMyAdmin** merupakan bagian untuk mengelola basis data MySQL yang ada dikomputer. Untuk membukanya dapat menggunakan *browser* lalu ketikkan alamat http://local*host*/phpMyAdmin. Halaman ini menampilkan semua database yang ada pada MySQL yang digunakan pada akplikasi web base dapat ditampilkan dan diolah. Gambar 4.7 menunjukkan Database RAPD yang digunakan dalam aplikasi ini yang memiliki 3 buah tabel yaitu Tabel User, Tabel List_rap, dan Tabel Komentar.

localhost ▸ rapd

Table	Records	Type	Size	Comments
komentar	1	InnoDB	16.0 KiB	Creation: Jun 10, 2011 at 02:45
list_rap	1	InnoDB	16.0 KiB	Creation: Jun 10, 2011 at 02:41
user	3	InnoDB	16.0 KiB	Tabel User Creation: Jun 10, 2011 at 02:35
3 table(s)	**5**	--	**48.0 KiB**	

Gambar 4.7 Tabel dalam Database RAPD

- **Kontrol Panel** yang berfungsi untuk mengelola layanan (*service*) XAMPP. Seperti menghentikan (*stop*) layanan, ataupun memulai (*start*). Gambar 4.8 merupakan tampilan dari Control Panel XAMPP.



Gambar 4.8. XAMPP control panel

4.2 Aplikasi Deteksi RAP Berbasis Web

Pembuatan Aplikasi berbasis Web terbagi menjadi 2 bagian yaitu bagian *client side Scripting* dan Aplikasi Web. *Client side Scripting* merupakan pemrograman dengan menggunakan bahasa *scritping* (java*Script* dan vb*Script*) yang dapat melakukan eksekusi di computer user dengan menggunakan *browser*.

Khusus pada penelitian ini *browser* yang digunakan adalah internet explorer dengan beberapa pertimbangan seperti (1) De facto Microsoft windows merupakan Operating Sistem yang paling banyak dipakai oleh pengguna di seluruh dunia, dan dapat dipastikan setiap windows by default mempunyai *browser* internet explorer, sehingga aplikasi deteksi RAP berbasis web dapat diakses oleh banyak user tanpa harus melakukan penginstalan program apapun di komputernya. (2) *Client side Scripting* berfungsi untuk menghitung RTT dari paket DNS dan DHCP yang akan digunakan sebagai parameter pada aplikasi ini, di windows program yang biasa digunakan untuk melakukan DNS lookup dan DHCP request adalah nslookup dan ipconfig, *Script* dapat dengan mudah melakukan eksekusi program nslookup dan ipconfig.

4.2.1 *Client Side Scripting*

Script ini akan melakukan eksekusi terhadap command nslookup.exe (DNS lookup) dan ipconfig.exe (DHCP request/renew) kemudian *Script* ini menghitung dan mencatat durasi waktu antara mulai dieksekusinya command tersebut dengan saat diterima respon dari command tersebut. Hal tersebut dilakukan secara berulang-ulang sejumlah n kali. (iterasi =n), durasi waktu inilah yang akan dianalisa sebagai Round Trip Time (RTT).

Saat *Station* terhubung ke AP atau RAP dan memperoleh koneksi internet maka dilakukan eksekusi *Script* dari interface *website* untuk menghitung RTT (DNS dan DHCP) sebanyak n kali, *Script* ini kemudian mengirimkan statistik dari data RTT tersebut ke web*server* untuk diolah lebih lanjut. Gambar 4.9 berikut menunjukkan pseudocode dari *client Side Scripting*.

```
1: For i = 1 to n Do
2: Start DHCP-Timer
3: execute ipconfig.exe
4: Stop DHCP-Timer
5: RTTDHCP = DHCP-Timer – (Tdata + Tdhcp-process)
6: Start DNS-Timer
6: execute nslookup.exe
7: Stop DNS-Timer
8: RTTDNS = DNS-Timer – (Tdata + Tdns-process)
9: End For
10: Filter Outlier
11:RTTDHCP= Rata-rata RTTDHCP
12 RTTDNS = Rata-rata RTTDNS
13: Δt = RTTDNS-RTTDHCP
14: σdhcp = STD RTTDHCP
15: σdns = STD RTTDNS
16: Send Δt, σdhcp, σdns to Webserver
```

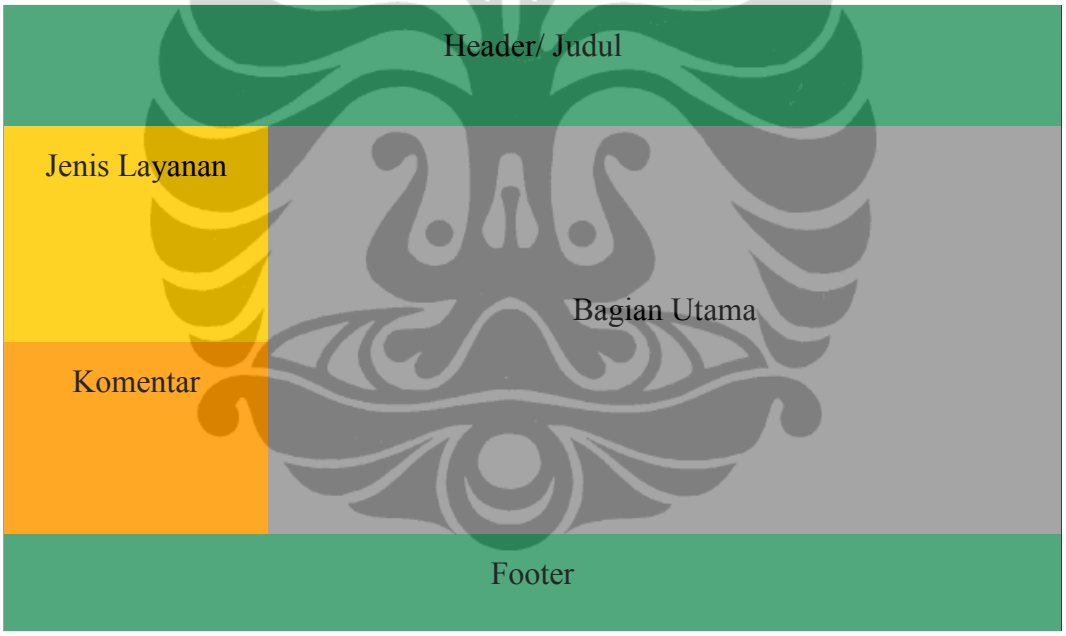
Gambar 4.9 Pseudocode *Client Side Scripting*

4.2.2 Aplikasi Web

Aplikasi Web: terbagi menjadi user web interface, RTT Handler, RAP detection, data store. Web interface memberikan antarmuka bagi user untuk melakukan pendeteksian terhadap akses point yang sedang digunakan. RTT Handler merupakan modul yang menerima data **Δt,** σ_{dhcp}, σ_{dns} yang dikirim oleh *client side Scripting*.

Web Interface menggunakan web CSS style dengan menggunakan template dari templateword.com yang sudah disesuaikan dengan kebutuhan yang ada. Layout dari webinterface terbagi menjadi beberapa bagian yaitu: Bagian Header/Judul, Bagian Layanan, Bagian Utama, Bagian Komentar dan Bagian Footer. Gambar 4.10 menunjukkan layout diagram dari web interface.

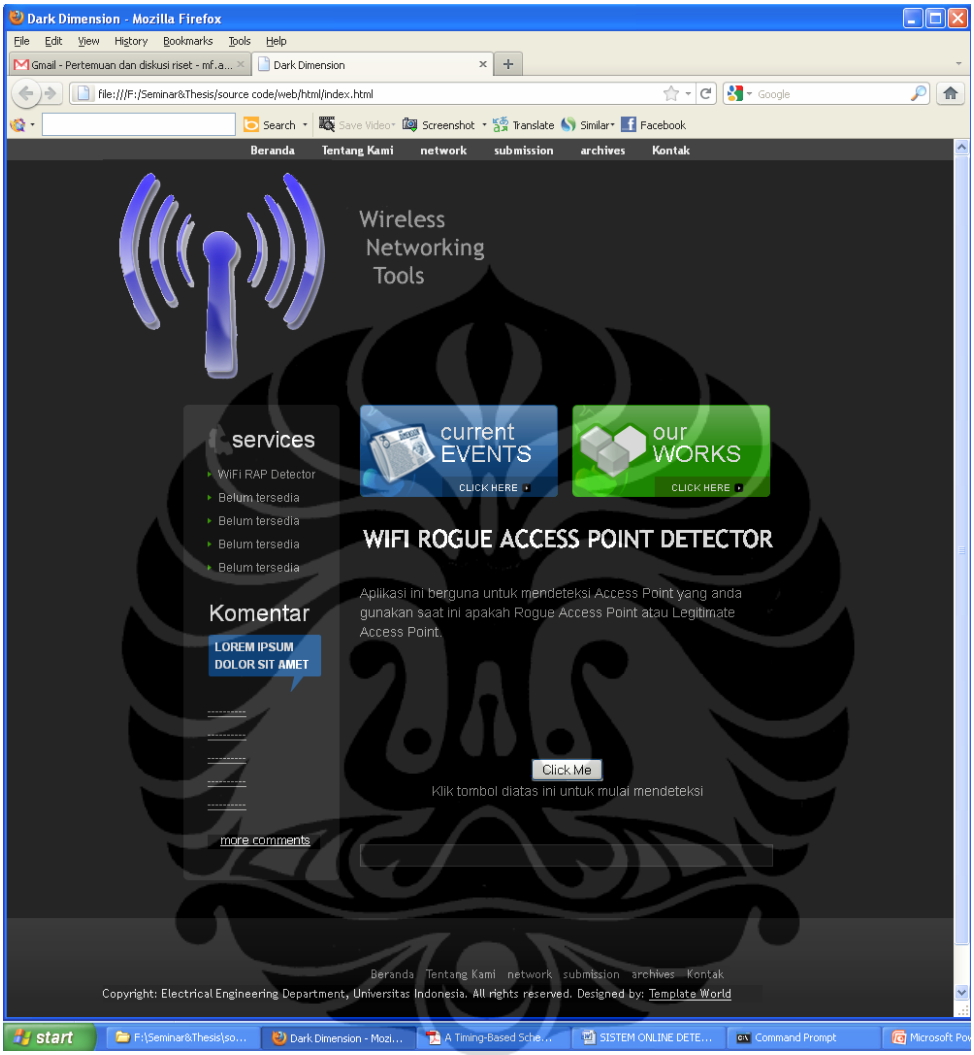
- Header / Judul berisi tentang Nama *Website* yang dibuat, dan hyperlink yang menghubungkan ke halaman beranda, tentang kami, network, kontak, dan Archieve.
- Jenis layanan memuat layanan yang disediakan bagi user internet oleh *website* ini
- Komentar merupakan bagian yang memuat komentar dari pengunjung *website* yang sudah menggunakan aplikasi ini
- Bagian utama berisi dari layanan yang akan dijalankan oleh user dalam hal ini deteksi RAP
- Footer berisi hyperlink seperti pada header dan juga berisi mengenai copyright dan lain-lain.



Gambar 4.10 Layout Diagram Web Interface

Layout diatas disusun dengan CSS Style supaya memudahkan dalam pengembangan kedepannya apabila ada fitur-fitur baru yang ditambahkan oleh *website* tersebut. Setelah Layout web sudah ditentukan maka kemudian diimplementasikan ke Web HTML dengan mengikuti acuan dari layout tersebut.

Gambar 4.11 menunjukkan hasil jadi dari homepage *website* yang dibuat untuk mendeteksi RAP.

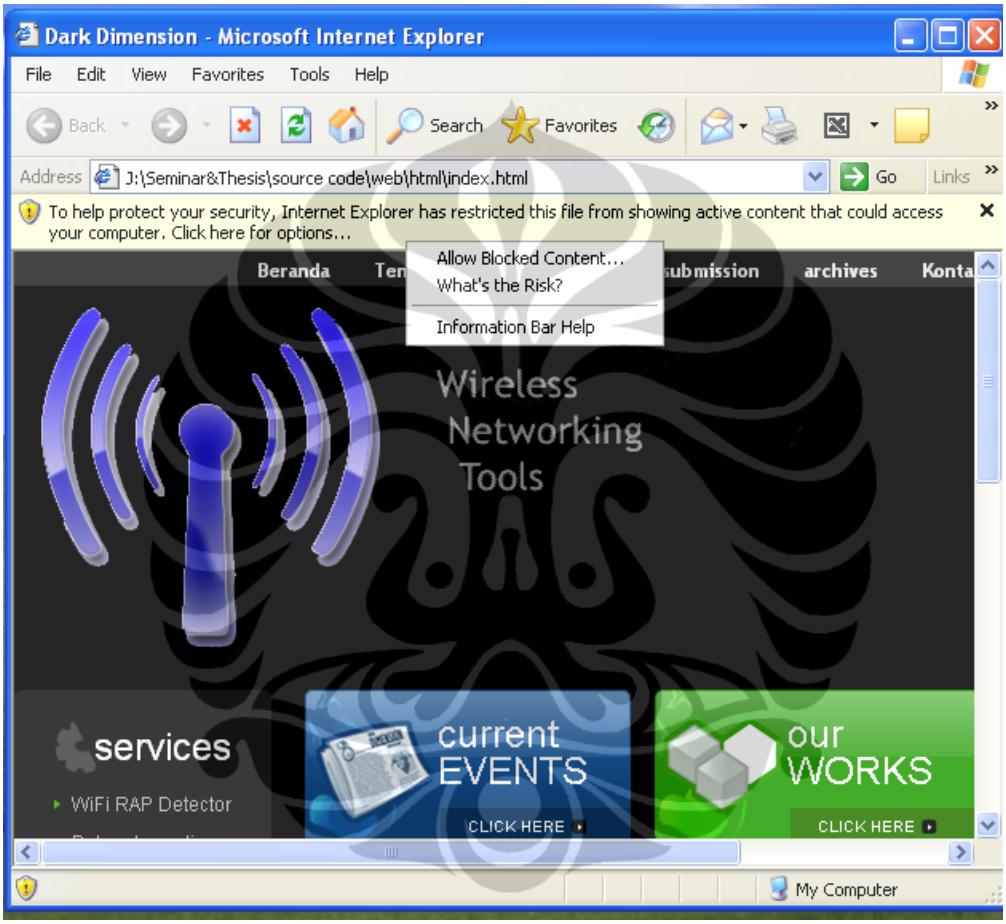


Gambar 4.11 Halaman Interface *Website* RAP Detektor

Dalam implementasinya Interface Web ini baru berfungsi dengan baik jika dijalankan dengan menggunakan *browser* Internet Explore, hal ini terkait dengan *client side Scripting* yang tidak dapat menghandle command ipconfig.exe dan nslookup.exe apabila dijalankan di *browser* selain internet exlporer seperti mozilla, opera dll.

Kekurangan lainnya adalah pada saat user mengakses *website* ini akan muncul *security warning popup* pada *browser* internet explorer bahwa *website* yang

sedang diakses kemungkinan mengandung *Script* yang membahayakan, hal ini memang wajar karena alasan untuk meningkatkan *security* pada sistem windows, oleh karena itu di web interface ini juga ada pemberitahuan ke user mengenai hal itu sehingga apabila muncul *security* warning, user memperbolehkan untuk menjalankan *Script* yang ada. Hal ini seperti tampak pada Gambar 4.12 berikut ini.



Gambar 4.12 *Security* Warning yang muncul pada *browser* IE

4.3 Pengujian dan Analisa

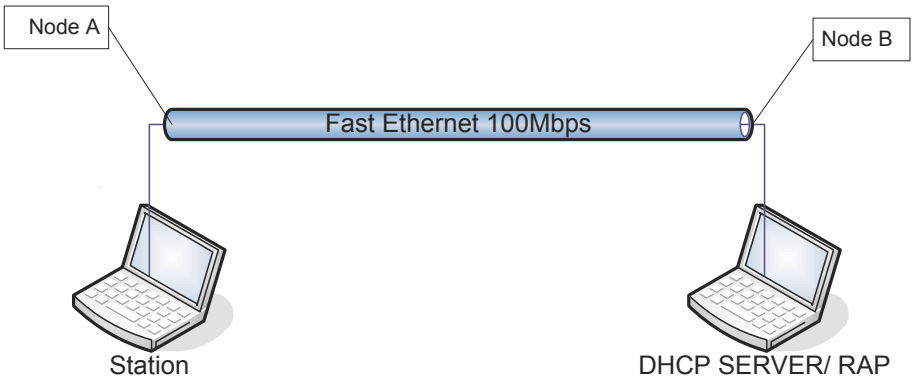
4.3.1 Setting dan Parameter Awal

Sebelum dilakukan pengujian terhadap system, maka harus ditentukan terlebih dahulu setting dan parameter-paramater yang akan dipakai dalam pengujian tersebut, agar pada saat pengujian diperoleh data yang memiliki acuan yang jelas sehingga memudahkan dalam pengolahan dan analisa data hasil pengujian. Setting dan parameter pada Sistem pada saat pengujian ditunjukkan Pada Table 4.1 berikut ini.

Tabel 4.1 Setting dan parameter pada Sistem

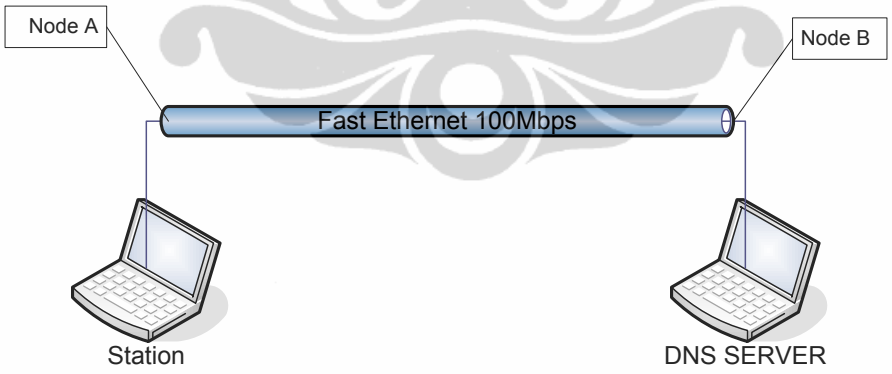
No	Protokol	802.11b	802.11g
1	BW WiFi	11 Mbps	54 Mbps
2	BW Ethernet	100 Mbps	100 Mbps
3	T_Process_DHCP	0,308365 s	0,308365 s
4	T_Process_DNS	0,074226 s	0,074226 s
5	T_Data_DHCP	0,089 ms	0,089 ms
6	T_Data_DNS	0,131 ms	0,131 ms

T_Process_DHCP adalah merupakan waktu rata-rata yang diperlukan oleh *Script* untuk melakukan DHCP request ke DHCP *server* dan menerima responnnya. Nilai T_Process_DHCP diperoleh dengan melakukan DHCP request ke DHCP *server* sebanyak n kali dan mengukur waktu kedatangan packet pada masing-masing node dengan menggunakan software Wireshark seperti terihat pada Gambar 4.13 berikut, baru kemudian diambil nilai rata-ratanya.



Gambar 4.13 Skema pengukuran T_Process_DHCP

Seperti halnya T_Process_DHCP pada Gambar 4.14 ditunjukkan skema pengukuran T_Process_DNS, dimana Process_DNS merupakan waktu rata-rata yang diperlukan *Script* untuk merequest DNS *Server* untuk memberikan respon terhadap DNS lookup request dari *Station* dan menerima respon tersebut. Nilai T_Process_DNS diperoleh dengan melakukan DNS lookup request ke DNS *server* sebanyak n kali dan mengukur waktu kedatangan packet pada masing-masing nde, kemudian diambil nilai rata-ratanya.

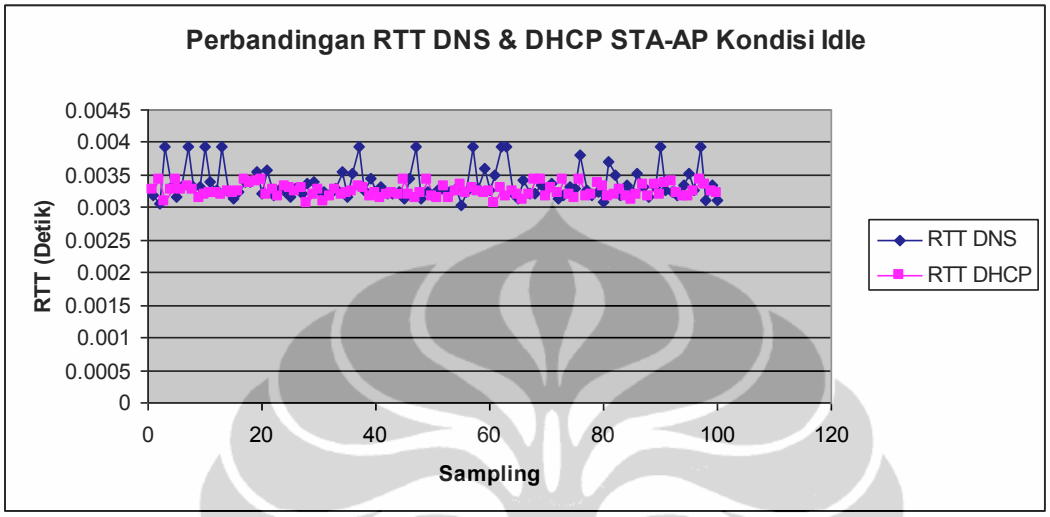


Gambar 4.14. Skema pengukuran T_Process_DNS

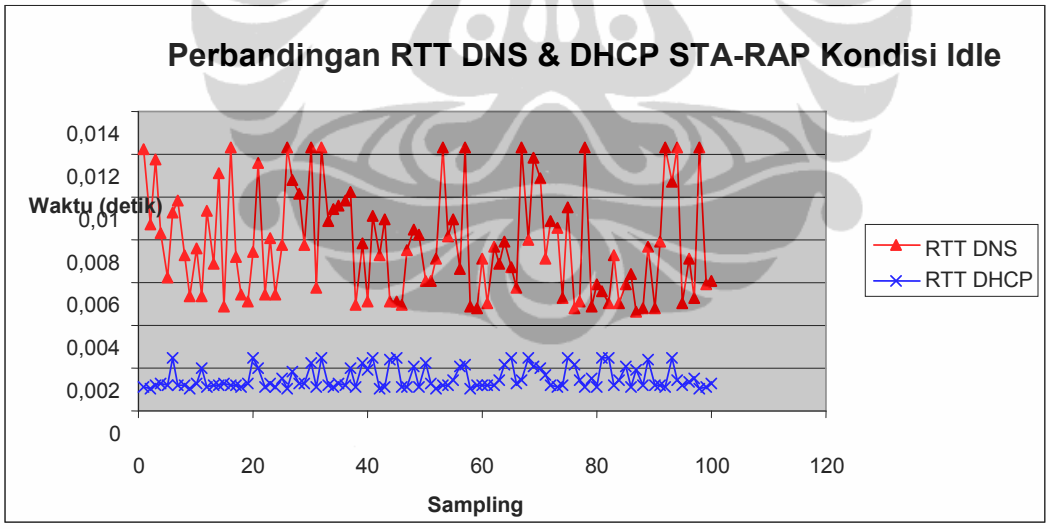
4.3.2 Penentuan ambang batas θ

Dalam implementasi Sistem Pendeteksi RAP berbasis Web ini diperlukan parameter ambang batas θ untuk menentukan apakah AP yang diuji merupakan sebuah *Legitimate AP* atau sebaliknya merupakan Rogue AP. Untuk menentukan

parameter ini dilakukan pengukuran pada *Testbed* dengan melakukan percobaan berulang-ulang untuk mengetahui nilai θ. Dari hasil percoabaan dan pengukuran sample maka diperoleh hasil untuk pengujian *Legitimate AP* seperti ditunjukkan pada Gambar 4.15 dan Rogue AP pada Gambar 4.16.



Gambar 4.15 Perbandingan RTT DNS dan RTT DHCP dari *Station* ke AP



Gambar 4.16 Perbandingan RTT DNS dan RTT DHCP dari *Station* ke RAP

Sesuai dengan perkiraan awal bahwa perbedaan RTT DNS dan RTT DHCP dari *Station* ke AP pada kondisi idle akan sangat kecil mengingat tidak adanya perbedaan hop antara trafik DNS dengan trafik DHCP, hal itu ditunjukkan pada

grafik pada gambar xx dimana letak koordinat RTT DHCP dan RTT DNS saling berimpitan sangat dekat.

Sedangkan pada pada grafik pada Gambar xx tampak jelas bahwa ada perbedaan jarak yang cukup terlihat antara kelompok koordinat RTT DNS dengan kelompok koordinat RTT DHCP, hal ini menunjukkan bahwa dengan adanya tambahan hop karena paket DNS harus melalui RAP dahulu baru menuju ke *Server* DNS maka terjadi penambahan waktu RTT untuk paket DNS, yang dipakai sebagai dasar pendeteksian RAP.

Parameter ambang batas θ digunakan untuk menentukan apakah AP yang diuji merupakan *Legitimate AP* atau RAP dimana $\Delta t < \theta < \Delta t'$. Pada Tabel 4.2 dan Tabel 4.3 ditunjukkan statistik dari hasil pengujian AP dan AP pada kondisi trafik idle.

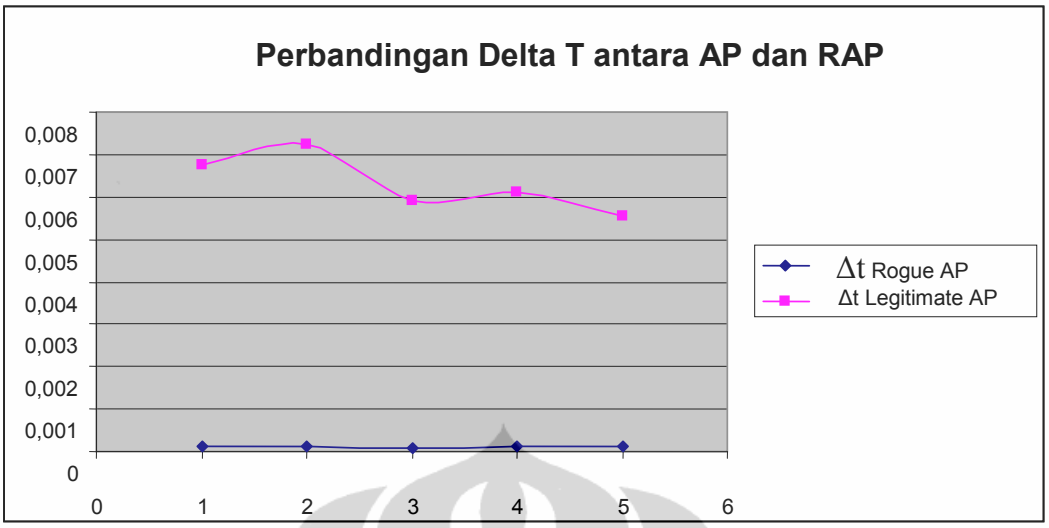
Tabel 4.2 Δt pada pengujian *legitimate* AP

No	Rata-rata RTT					
1.	RTT_{DHCP}	0,003277	0,00322	0,00323	0,003245	0,003244
2.	RTT_{DNS}	0,003411	0,003342	0,003326	0,003355	0,003376
3	Δt (2-1)	0,000134	0,000121	9,65E-05	0,00011	0,000132

Tabel 4.3 Δt pada pengujian Rogue AP

No	Rata-rata RTT					
1.	RTT_{DHCP}	0,001347	0,001523	0,001548	0,00164	0,001567
2.	RTT_{DNS}	0,008087	0,008778	0,007475	0,007766	0,007114
3.	Δt' (2-1)	0,006739	0,007255	0,005926	0,006126	0,005547

Dari Tabel 4.2 dan 4.3 terlihat bahwa pada *Legitimate AP* maka Δt paling besar tidak lebih dari 0,00014 detik (0,14 milidetik). Sedangkan pada pengujian rogue AP maka diperoleh Δt paling kecil tidak kurang dari 0,005547 detik (5,5547 milidetik). Pengambilan data dilakukan untuk kondisi trafik idle, sehingga merupakan kondisi paling bagus untuk RAP dalam mentransmisikan paket DNS dari *Station* ke *Legitimate AP*.



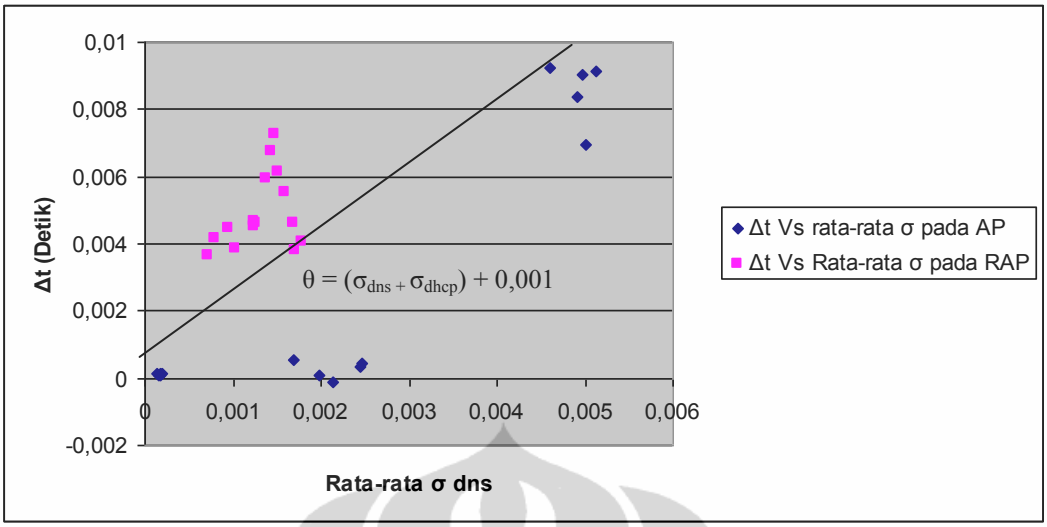
Gambar 4.17 Perbandingan Δt pada AP dan RAP

Jika digabungkan antara Δt pada pengujian Rogue AP dengan *Legitimate AP* akan terlihat seperti grafik pada Gambar 4.17. Terlihat bahwa Δt pada legtimate AP memiliki nilai rata-rata dibawah 1 milidetik, dan hal ini sesuai dengan persamaan 2.4 dimana Δt adalah T_{Kabel} atau waktu yang diperlukan untuk mentransmisikan paket DNS pada jaringan LAN ethernet dari AP ke *Server* DNS. Sedangkan Δt pada pengujian Rogue AP memiliki nilai rata-rata diatas 5 milidetik dan ini merupakan waktu yang diperlukan oleh RAP untuk meneruskan paket DNS ke DNS *Server*, sehingga untuk kondisi idle dapat diambil nilai θ sekitar 1 milidetik.

Dari hasil pengukuran terhadap Δt dan standar deviasi RTTDNS (σ_{dns}) pada AP maupun RAP pada semua kondisi trafik wireless *idle*, sedang, dan saturasi diperoleh grafik seperti terlihat pada Gambar 4.18. Tampak bahwa hampir semua Δt pada RAP menempati posisi diatas garis lurus sedangkan pada AP sebagian besar berada dibawahnya dan sedikit yang berada diatas garis tersebut. Hal ini menunjukkan bahwa nilai θ harus berubah secara dinamik mengikuti perubahan nilai σ_{dns}. Dengan demikian nilai ambang batas θ dapat kita asumsikan sebagai berikut:

$$\theta = (\sigma_{dns} + \sigma_{dhcp}) + 0{,}001 \text{ (detik)} \quad \text{..... (4.1)}$$

Parameter inilah yang dipakai oleh aplikasi untuk membedakan antara AP dan RAP.



Gambar 4.18 Hubungan Δt dengan σ_{dns} pada kondisi trafik yang bervariasi.

4.3.3 Skenario Pengujian

Pengujian terhadap sistem dilakukan dengan menggunakan beberapa skenario yang berbeda-beda parameternya, agar diperoleh hasil pengujian yang sesuai dengan kondisi yang real yang ada di lapangan. Dari beberapa skenario yang ada diambil skenario yang diperkirakan paling mempengaruhi fluktuasi dari pewaktuan RTT yaitu:

- Kecepatan Transmisi Data

  RTT berbanding terbalik dengan kecepatan transmisi data, jika kecepatan transmisi data besar maka biasanya RTT yang diperoleh akan kecil, demikian sebaliknya.

- Trafik Wireless

  RTT juga dipengaruhi oleh trafik wireless yang terjadi antara *Station* dengan RAP dan *Station* dengan AP. Pendeteksian RAP akan lebih sulit jika kondisi trafik jaringan tidak dalam kondisi sibuk mengingat banyak terjadi antrian paket di udara sehingga menyulitkan untuk menghitung RTT.

- Beban Kerja AP

  AP dengan beban kerja yang tinggi pada umumnya juga membutuhkan waktu untuk memproses paket yang keluar masuk, sehingga semakin besar beban

kerja AP akan menyebabkan bertambahnya RTT yang akan dicatat oleh sistem pendeteksi RAP.

4.3.3.1 Kecepatan Transmisi Data

Untuk mengetahui pengaruh kecepatan transmisi data yang digunakan dari RAP ke AP maka dilakukan tes dan pengukuran dari RAP ke AP. Pertama kali RAP disetting untuk menggunakan 802.11g dengan kecepatan transmisi Auto rate adaptation pada kondisi trafik idle. Kemudian pada kondisi trafik yang sama dilakukan tes lagi namun dengan menggunakan kecepatan transmisi data fixed 54 Mbps. Pengukuran dilakukan dengan n=100 karena trafik idle maka parameter θ adalah 1 milidetik.

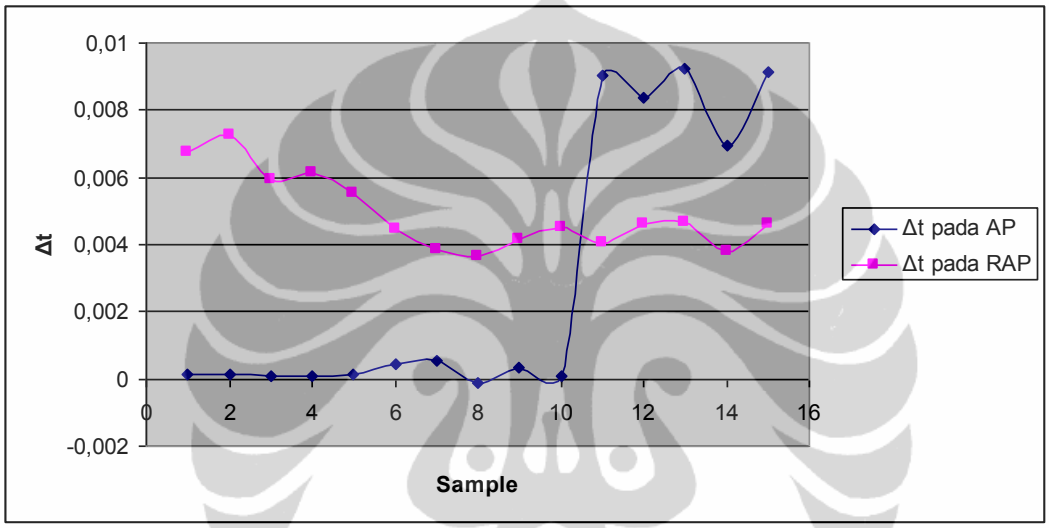
Tabel 4.4 Pengaruh Kecepatan Transmisi pada Δt

	Rata-rata RTT setelah di filter					RAP
DHCP	0,001658	0,001837	0,00212	0,001764	0,00185	Rate auto
DNS	0,008495	0,006881	0,007182	0,006815	0,008392	
Δt	0,006836	0,005044	0,005062	0,005051	0,006542	
DHCP	0,001733	0,001749	0,002174	0,001954	0,002164	Rate 54 Mbps
DNS	0,007175	0,009018	0,008067	0,008018	0,008715	
Δt	0,005443	0,007269	0,005893	0,006064	0,006552	

Dari Tabel 4.4 terlihat bahwa meskipun RAP disetting untuk menggunakan kecepatan paling maksimal akan tetapi Δt masih lebih besar dari θ sehingga masih dapat terdeteksi sebagai RAP. Penggunaan Fixed rate tidak memberikan keuntungan berarti bagi RAP mengingat dengan menggunakan rate auto RAP dapat dengan cepat menggunakan kecepatan terbaik yang mungkin diperolehnya. Bahkan penggunaan Fixed dapat menyebabkan penurunan kinerja RAP dikarenakan pada kondisi trafik berfluktuasi akan ada paket yang didrop, hal ini terlihat pada nilai Δt yang lebih besar.

4.3.3.2 Trafik Wireless

Dengan menggunakan notebook yang diinstall dengan software Iperf dapat digunakan sebagai trafik generator yang akan dipakai untuk mengatur besarnya trafik wireless yang ada. Pada pengujian dibuat pengelompokan trafik berdasarkan utilisasi kanal pada wifi yaitu utilisasi kanal 0 – 10% digolongkan sebagai trafik idle, 15 – 50% digolongkan sebagai trafik medium, dan 60 – 100% digolongkan sebagai trafik saturasi.



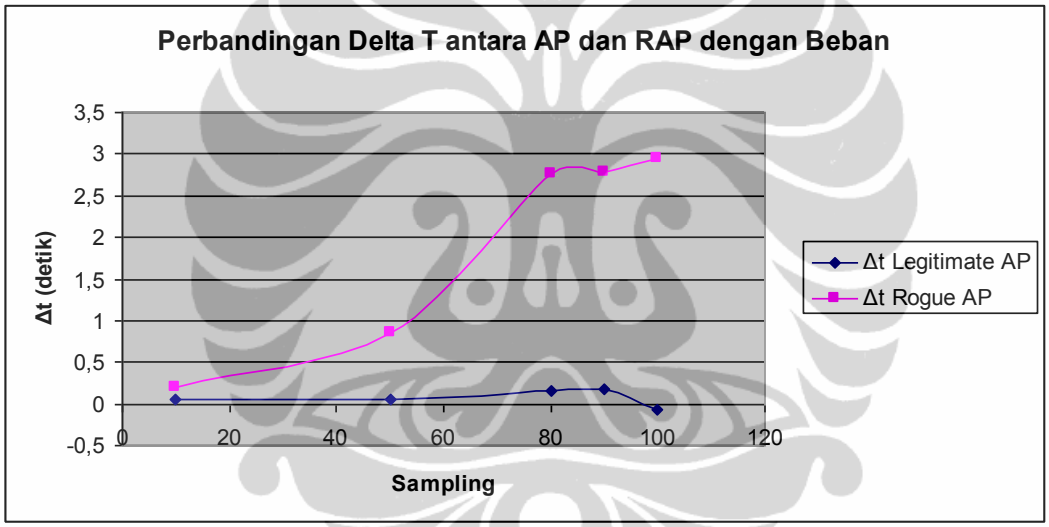
Gambar 4.19 Perbandingan Δt antara AP dan RAP pada berbagai kondisi Trafik

Pada Gambar 4.19 terlihat bahwa pada kondisi trafik idle sampai pada trafik sedang (sample 1-10) masih terlihat jelas perbedaan yang cukup signifikan antara Δt pada pengujian AP dengan Δt pada pengujian RAP. Sedangkan pada kondisi trafik saturasi terlihat jelas bahwa Δt pada AP bergerak melebihi Δt pada RAP dan akhirnya pada kondisi saturasi Δt AP akan terus melebihi Δt pada RAP.

Dengan demikian dapat diambil kesimpulan bahwa kemungkinan untuk mendeteksi RAP pada kondisi trafik idle dan sedang adalah cukup efektif sedangkan pada kondisi trafik saturasi kemungkinan besar akan terjadi kesalahan pendeteksian baik itu berupa *false positif* maupun *false negatif*.

4.3.3.3 Beban Kerja AP

Sebuah AP yang akan dijadikan sebagai akses bagi RAP pada kenyataannya tidak bisa terlepas dari *Station-Station* yang mengakses AP tersebut yang akan menyebabkan bervariasinya beban yang berpengaruh pada pengiriman paket data dari AP yang harus menunggu paket data yang lain terkirimkan terlebih dahulu. Pengujian ini bertujuan untuk mengetahui pengaruh beban kerja pada AP terhadap Δt. Pada pengujian ini dilakukan pemberian beban pada AP dengan menggunakan Genator Trafik yang secara terus menerus mentransfer data melalui AP tersebut, dengan beban ringan (1<Mbps), medium (5 Mbps) dan berat (>14 Mbps) secara berurutan.



Gambar 4.20 Efek Beban pada AP terhadap Delta T

Seperti tampak pada Gambar 4.20 hasil pengujian ternyata memperlihatkan bahwa terjadi variasi yang cukup signifikan pada Δt pada saat AP diberikan beban yang bervariasi. Pada beban yang berat maka Δt yang dihasilkan oleh RAP mengalami peningkatan yang cukup signifikan dimana pada beban puncak Δt mencapai hampir 3 detik, sedangkan pada beban sedang terjadi penurunan Δt menjadi sekitar 0,5 - 1 detik dan akhirnya pada kondisi beban ringan Δt mendekati 0,1 detik. Sebaliknya pada pengujian *Legitimate AP* tampak bahwa pengaruh beban pada AP tidak terlalu berpengaruh pada variasi Δt, hal ini dikarenakan pada *Legitimate AP* pengiriman paket DNS dan DHCP hanya terjadi pada satu hop

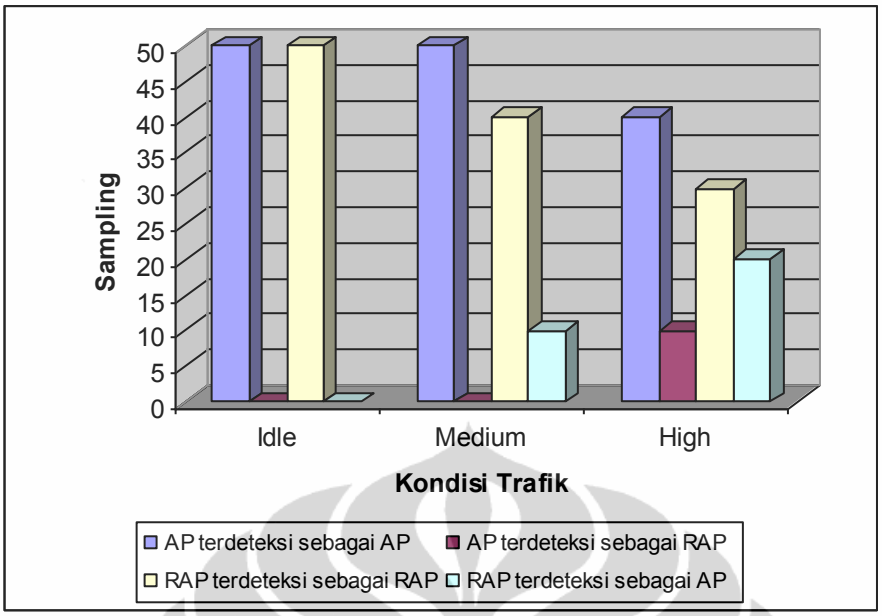
yaitu antara *Station* ke AP sehingga apabila terjadi variasi beban pada AP mengakibatkan paket DNS dan DHCP keduanya mengalami delay yang sama variasinya. Berbeda dengan pada RAP dimana paket DHCP tidak dilayani oleh AP namun oleh RAP sendiri sehingga pada saat ada variasi beban pada AP maka yang terkena pengaruhnya hanya paket DNS saja sehingga Δt akan mengikuti delay sesuai delay paket DNS yang dikirimkan melalui AP.

4.3.4 Akurasi Pendeteksian

Setelah parameter ambang batas diperoleh dan dijelaskan pada Sub Bab 4.3.2, baru kemudian parameter tersebut di masukkan kedalam modul RAP detektor yang ada pada Aplikasi yang diupload di Web*server*. Pengujian dilakukan untuk mengetahui akurasi dari sistem pada saat dijalankan pada 3 kondisi trafik yang ada yang sudah diskenariokan yaitu idle, medium, dan high. Pada pengujian dilakukan 100 kali sampling masing-masing 50 sampling dengan sasaran uji AP dan 50 sampling dengan sasaran uji RAP, dilakukan pada 3 kondisi trafik tersebut. Setiap pengujian menggunakan jumlah iterasi n = 100 dan dilakukan pengulangan sebanyak 10 kali, detail pengujian akurasi sistem dapat dilihat pada tabel pada lampiran 1.

Gambar 4.21 menunjukkan grafik hasil pengujian terhadap sistem. Dari hasil pengujian terhadap aplikasi pada kondisi trafik Idle maka diperoleh tingkat akurasi 100% dimana tidak pernah terjadi kesalahan pendeteksian baik untuk AP maupun RAP. Sedangkan pada kondisi trafik medium pada pendeteksian AP tidak terjadi kesalahan namun pada pendeteksian RAP terjadi kesalahan pendeteksian sebanyak 10 kali yaitu RAP dideteksi sebagai AP atau dalam istilah lain terjadi 10% false negatif dengan demikian tingkat akurasi sistem mencapai 90%.

Pada kondisi trafik high terjadi peningkatan false negatif dimana jumlah RAP yang dideteksi sebagai AP meningkat menjadi 20% dan pada sasaran AP terjadi kesalahan pendeteksian 10% atau false positif 10% sehingga akurasi sistem mencapai 70%. Hal ini terjadi karena pada trafik high terjadi variasi yang cukup besar dari ketiga parameter yaitu Δt, σ_{dns} , σ_{dhcp} akibat banyak terjadinya paket delay dan retransmision.



Gambar 4.21 Tingkat Akurasi Sistem Pada Berbagai Kondisi Trafik

BAB 5
KESIMPULAN

Dari hasil pengujian dapat disimpulkan bahwa penggunaan sistem pendeteksi *rogue access point* dengan aplikasi berbasis web maka user dapat dengan mudah mendeteksi keberadaan RAP tersebut tanpa melibatkan administrator jaringan.

Dari hasil pengujian dan analisa data yang diperoleh dapat disimpulkan beberapa hal sebagai berikut:

- Kecepatan transmisi data pada WiFi tidak terlalu berpengaruh pada proses pendeteksian RAP
- Akurasi pendeteksian RAP oleh sistem dipengaruhi oleh trafik pada jaringan WiFi dan dengan variasi beban pada AP yang dijadikan gateway oleh RAP, semakin besar trafik WiFi dan beban AP maka semakin berkurang keakuratan sistem untuk mendeteksi RAP.
- AP yang memiliki beban kerja maksimal mengakibatkan terjadinya variasi Δt yang cukup signifikan pada pengujian RAP.
- Tingkat akurasi pendeteksian sistem mencapai 100% pada kondisi trafik idle, kemudian menurun menjadi 90% pada kondisi trafik medium dan turun lagi menjadi 70% pada kondisi trafik high.

Mengingat masih terbatasnya pemakaian aplikasi ini pada sistem windows diharapkan kedepannya ada pengembangan sistem pendeteksi RAP sejenis ini sehingga dapat mensupport berbagai Operating Sistem yang ada serta juga dengan memberikan tingkat keakuratan pendeteksian yang lebih tinggi.

DAFTAR REFERENSI

[1] Watkins, L., Beyah, R., Corbett, C., "A Passive Approach to Rogue Access Point Detection", IEEE GLOBECOM Washington DC, USA, 26-30 November 2007.

[2] Hao Han, Bo Shen, Chiu C. Tan, Qun Li., Sanglu Lu., "A Measurement Based Rogue AP Detection Scheme", IEEE INFOCOM, Rio de Janeiro, 19-25 April 2009.

[3] Godber, A., and Dasgupta, P., "Countering Rogues in *Wireless Networks*", DARPA/Spawar, AFOSR and NSF 2003.

[4] Y. Song , C. Yang, and G. Gu., "Who Is Peeping at Your Passwords at Starbucks? - To Catch an Evil Twin Access Point", IEEE/IIFIP International Conference on Dependable Systems & Networks (DSN), Chicago,USA, 28 Juni - 1 Juli 2010.

[5] Songrit Srilasak, Kitti Wongthavarawat and Anan Phonphoem, "Integrated Wireless Rogue Access Point Detection and Counterattack System ", International Conference on Information *Security* and Assurance, Hanwha Resort Haeundae, Busan, Korea, 24 – 26 April 2008.

[6] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell., "Detecting 802.11 MAC layer spoofing using received signal strength", IEEE INFOCOM, Phoenix, AZ, USA, 15 – 17 April 2008.

[7] S. Jana and S. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews", Mobicom, San Francisco, California, USA, 14 – 19 September 2008.

[8] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures", Mobicom, San Francisco, California, USA, 14 – 19 September 2008.

[9] S. Shetty, M. Song, and L. Ma, "Rogue access point detection by analyzing network traffic characteristics", Milcom, Orlando, Florida, 29 – 31 October 2007

Lampiran 1. Tabel Pengujian Akurasi Sistem Pendeteksi RAP dengan Aplikasi Berbasis Web

No	N=100	AP/AP	AP/RAP	RAP/RAP	RAP/AP
1	Idle	49	1	50	0
	Medium	47	3	39	11
	High	38	12	32	18
2	Idle	50	0	48	2
	Medium	49	1	41	9
	High	39	11	31	19
3	Idle	48	2	50	0
	Medium	49	0	40	10
	High	39	11	31	19
4	Idle	49	1	50	0
	Medium	50	0	43	7
	High	40	10	27	23
5	Idle	50	0	48	1
	Medium	48	0	39	11
	High	42	8	29	21
6	Idle	49	1	48	2
	Medium	49	1	42	8
	High	41	9	30	20
7	Idle	49	1	50	0
	Medium	49	1	41	9
	High	44	6	29	21
8	Idle	49	1	47	3
	Medium	50	0	40	10
	High	42	8	27	23
9	Idle	49	1	50	0
	Medium	48	1	39	11
	High	39	11	33	17
10	Idle	49	1	50	0
	Medium	48	2	38	12
	High	38	12	32	18
		AP/AP	AP/RAP	RAP/RAP	RAP/AP
Rata-rata	Idle	49.1	0.9	49.1	0.8
	Medium	48.7	0.9	40.2	9.8
	High	40.2	9.8	30.1	19.9