e-ISSN: 2252-7036
Vol.2 No.3 2017: 105-111

# Pengujian dan Analisis Keamanan WPA2 dan Signal Strength pada Router Berbasis OpenWrt

Syarif Maulana[#1], Teuku Yuliar Arif[#2], Rizal Munadi[#3]

[#]*Jurusan Teknik Elektro Dan Komputer, Fakultas Teknik Universitas Syiah Kuala*
*Jl. Tgk. Syech Abdul Rauf No. 7, Darussalam, Banda Aceh 23111 Indonesia*

[1]syarifmaulana.id@gmail.com
[2]yuliar@unsyiah.ac.id
[3]rizal.munadi@unsyiah.ac.id

*Abstrak* — **Seiring dengan perkembangan teknologi, keamanan suatu perangkat merupakan hal penting yang menjadi perhatian khusus. Salah satunya adalah keamanan jaringan WiFi, dengan sistem proteksi WiFi Protected Access (WPA2) yang menggunakan enkripsi Temporal Key Integrity Protocol (TKIP) dan Advanced Encryption Standard (AES). Sistem keamanan WPA/WPA2 sendiri memiliki kerentanan terhadap serangan seperti dictionary attack. Selain itu, keandalan suatu jaringan yang dipancarkan oleh router dapat diukur salah satunya berdasarkan parameter kuat sinyal (signal strength). Signal strength berkisar antara -10 dBm hingga -95 dBm tergantung pada jarak siaran WiFi antara perangkat router dan pengguna. Beberapa router memiliki kekurangan yang bisa diminimalisir dengan mengganti firmware router yang lebih fungsional, seperti OpenWrt. Oleh karena itu, pada penelitian ini dilakukan pengujian keamanan WPA2 pada router OpenWrt dan melihat pengaruh signal strength pada router OpenWrt pada saat sinyal kuat, sedang, dan rendah. Hasil penelitian menunjukkan bahwa WPA2 OpenWrt masih dapat ditembus selama password yang digunakan terdapat pada wordlist dan signal strength tidak berpengaruh terhadap serangan, melainkan terhadap waktu.**

***Kata Kunci* — router, WiFi, WPA2, dBm, TKIP, AES, OpenWrt, aircrack, wordlist.**

## I. PENDAHULUAN

Sistem keamanan *Wireless Equivalent Privacy* (WEP) yang lama membutuhkan transmisi data yang lebih ringan dan kuat, karena proses enkripsi yang lebih sederhana daripada enkripsi pada mode *Wireless Protected Access* (WPA). Pada WEP, yang dipakai adalah algoritma enkripsi *Rivest Chiper* (RC4) dengan panjang kunci 40 bit**.** Sedangkan pada WPA menggunakan TKIP RC4 dengan proses enkripsi algoritma enkripsi RC4 dengan *Temporal Key Integrity Protocol* (TKIP) dan *message integrity check*, memiliki kunci enkripsi 64 bit atau 128-bit yang harus dimasukkan secara manual, dan pada WPA2 menggunakan sistem enkripsi *Advanced Encryption System* (AES) dengan ukuran kunci 128 bit, 192 bit, dan 256 bit, dan standar protokol *Counter Mode CBD-MAC Protocol* (CCMP) yang lebih aman dari keduanya. Pada saat pengenkripsian paket oleh WEP, terdapat penambahan inisiasi pada *secret key* sebelum kunci dimasukkan ke dalam RC4, yang menunjukkan bahwa tiga bit pertamanya membawa *secret key* pada setiap paket.

Pada WPA/WPA2, kunci enkripsi berupa *temporal key* didapat dari proses *four way handshake* yang menjalankan *sequence counter* untuk mengamankan terhadap serangan berulang [1].

Kualitas suatu sinyal jaringan WiFi ditentukan berdasarkan beberapa parameter, diantaranya kuat sinyal (*signal strength*), *delay*, *throughput*, dan *packet loss*. Kuat sinyal WiFi ditunjukkan oleh satuan level daya dengan referensi daya 1 mW, yaitu dBm. Rentang tinggi hingga rendahnya kekuatan sinyal WiFi berkisar antara -10 dBm hingga -95 dBm [2].

Selain menggunakan sistem operasi *router* bawaan sebagai penghubung antar jaringan, terdapat alternatif lain *firmware router* pihak ketiga seperti OpenWRT. OpenWRT merupakan *embedded firmware* yang digunakan untuk mengatur konfigurasi router secara bebas dan mendukung sistem enkripsi WEP, WPA/WPA2, dan 802.11i (WPA Enterprise) [3].

Penelitian tugas akhir ini berdasarkan informasi resmi yang dikeluarkan oleh OpenWRT, dinyatakan bahwa enkripsi khusus pada WPA sudah tidak aman dan tidak didukung lagi, tetapi enkripsi yang berlaku pada WPA2 masih aman. Selain itu, dengan menggunakan *default router* yang berbeda dari umum, dalam hal ini OpenWRT, maka patut dijadikan sebagai salah satu alasan pengujian. Pengujian dilakukan untuk mengetahui bagaimana pengaruh kuat sinyal atau *signal strength* terhadap serangan serangan *dictionary attack* pada keamanan WPA2 yang menggunakan OpenWRT sebagai *default router*, pengujian dilakukan dengan *tool aircrack-ng*.

## II. DASAR TEORI

### A. Router

Sebuah *router* mentransmisikan informasi dari satu jaringan ke jaringan yang lain melalui sebuah jaringan internet menuju tujuannya melalui sebuah proses yang disebut sebagai routing. Router hampir sama dengan Bridge namun memiliki kelebihan, router akan mencari jalur yang terbaik untuk mengirimkan sebuah pesan yang berdasakan atas alamat tujuan dan alamat asal [4]. Proses routing suatu router beroperasi pada layer 1, 2 dan 3 pada OSI layer, yaitu *physical*, *data link*, dan *network*. Suatu router terdiri dari [5]:

a. *Central processing unit* (CPU), mengeksekusi instruksi sistem operasi.
b. *Random Access Memory* (RAM), menyimpan instruksi dan data CPU.

e-ISSN: 2252-7036
Vol.2 No.3 2017: 105-111

c. *Read Only Memory* (ROM), menyimpan sistem instruksi *boot.*
d. *Flash*, menyimpan proses pada RAM selama *bootup*.
e. *NVRAM*, lokasi file konfigurasi tersimpan.

### *B. WiFi*

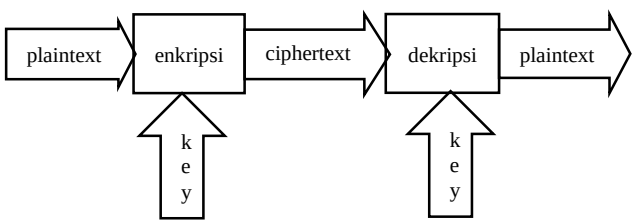
*Wireless Fidelity* (WiFi) adalah teknologi nirkabel berstandar *Institute of Electrical and Electronics Engineers* (IEEE) 802.11 yang menyediakan layanan internet tinggi bagi perangkat yang terhubung melalui jaringan komputer. WiFi menggunakan set *Media Access Control* (MAC) dan berada pada layer fisik untuk mengimplementasikan komunikasi komputer *Wireless Local Area Network* (WLAN) di frekuensi 2.4 GHz, 3.6 GHz, 5 GHz, dan 6 GHz [6]. WiFi mengadopsi berbagai teknologi enkripsi untuk kemanan jaringannya, diantaranya adalah WEP, WPA, dan WPA2. Jaringan wifi menggunakan *identifier* untuk dapat dihubungi oleh setiap perangkat yang memerlukan akses, yang disebut dengan *Service Set Identifier* (SSID). SSID dikonfigurasikan oleh perangkat jaringan dan mentransmisikan paket ke penerima.

TABEL I
JENIS DAN SPESIFIKASI IEEE 802.11 [7]

| ***802.11*** | ***Spesifikasi*** |
|---|---|
| 802.11a | Beroperasi pada pita frekuensi 5 GHz dan mendukung datarate hingga 54 Mbps. |
| 802.11b | Beroperasi pada pita frekuensi 2,4 GHz dan mendukung peningkatan data rate sampai dengan 11 Mbps. |
| 802.11g | Beroperasi pada pita frekuensi 2.4 GHz dan mendukung datarate sampai dengan 54 Mbps dan |
| 802.11n | Beroperasi pada pita frekuensi 2.4 GHz dan 5GHz, memiliki datarate mencapai 100 Mbps. |
| 802.11ac | Memiliki kinerja teknologi jaringan area lokal nirkabel mencapai hingga 1 Gbps. |

### *C. Sistem Keamanan*

Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematis yang berhubungan dengan keamanan informasi, misalnya keabsahan, integritas data, dan autentikasi data. Kriptografi memberikan keamanan informasi dan teknik-tekniknya. Kerahasian data yang dijaga oleh kriptografi dilakukan dengan transformasi data *plaintext* ke dalam bentuk sandi atau *ciphertext.*




Gambar 1 Proses Enkripsi dan Dekripsi

Pada kriptografi terdapat dua cara transformasi, yaitu enkripsi (*encryption*) dan dekripsi (*decryption*). Enkripsi adalah pentransformasian data *plaintext* menjadi *ciphertext*. Sedangkan dekripsi adalah pentransformasian *ciphertext* yang dikirimkan menjadi *plaintext*. Pengirim (*sender*) melakukan pengiriman *ciphertext* kepada penerima (*receiver*). Kemudian supaya bisa dikenali, maka *ciphertext* ditransformasikan kembali menjadi *plaintext* [8].

Tujuan dasar kriptografi adalah [9]:

a. Kerahasiaan (*confidentiality*), menjaga isi informasi agar hanya dapat digunakan oleh pemilik otoritas.
b. Integritas data (data integrity), penjaminan atas keaslian pesan dari penyisipan, penghapusan, dan perubahan oleh pihak yang tidak berhak.
c. Autentikasi (*authentication*), identifikasi pihak yang berkomunikasi harus dikenali, beserta sumber pesan dan waktu pengiriman.

Non-repudiasi (*non-repudiation)*, mencegah penangkalan pengiriman pesan oleh pengirim dan penerimaan pesan oleh penerima. Enkripsi bertujuan untuk memastikan pihak tersebut dapat membaca dan mengakses data dengan menggunakan kunci dekripsi. Jaringan WiFi menggunakan sistem enkripsi WEP, WPA, dan WPA2.

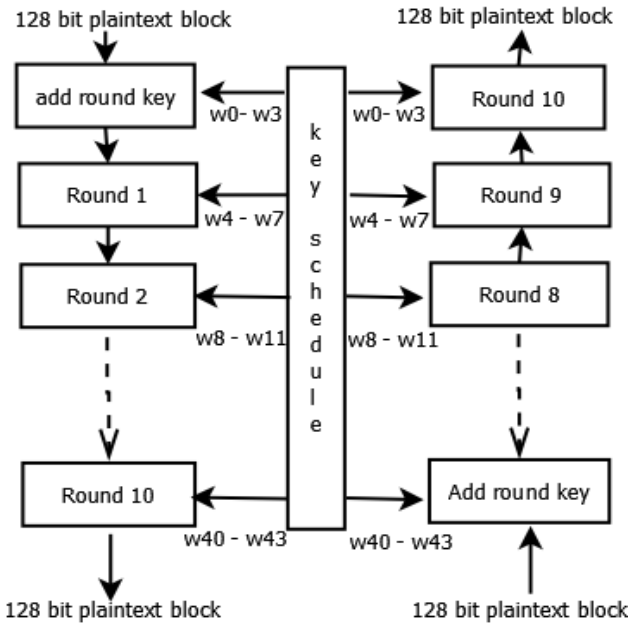
### *D. WPA*

WPA merupakan singkatan dari *WiFi Protected Access*, adalah protokol keamanan dan sertifikasi yang digunakan untuk mengamankan jaringan komputer. WPA dikenalkan pada tahun 2003 dan kemudian pada tahun 2004 terdapat pembaruan dengan nama WPA2, keduanya juga merujuk pada nama IEEE 802.11i standard. WPA dan WPA2 merupakan pengganti dari sistem enkripsi WEP sebelumnya yang dianggap sudak tidak aman. Pada WPA2 ada dua jenis autentikasi, *personal model authentication* yang menggunakan *Pre-Shared Key* (PSK) dan *Enterprise* model yang menggunakan *Extensible Authentication Protocol* (EAP) merujuk pada WPA-802.1X. Autentikasi WPA2-PSK yang terjadi antara klien dan *access point* dilakukan dengan menggunakan enkripsi kunci 256 bit dan tidak memerlukan server autentikasi. Kunci terdiri dari 8 hingga 63 karakter frasa *plaintext* yang diinput pada klien dan *access point* (AP) [10].

### *E. AES*

WPA2 menggunakan algoritma enkripsi *Advanced Enryption Standard* (AES). AES terbagi menjadi tiga: AES-128 bit, AES-192 bit, dan AES-256 bit. Dengan blok *chipertext* simetris yang melakukan enkripsi dan dekripsi, dan sistem permutasi dan subtitusi (P-Box dan S-Box). Terdapat empat jenis transformasi *bytes* pada algoritma AES, diantaranya *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Transformasi dimulai pada *AddRoundKey*, proses ini disebut dengan *round function* [10].

e-ISSN: 2252-7036
Vol.2 No.3 2017: 105-111




Gambar 2 Diagram *encryption* dan *decryption* AES

Pada AES, enkripsi terdiri dari 10 ronde dengan pemrosesan 128 bit kunci, 12 ronde untuk 192 bit kunci, dan 14 ronde untuk 256 bit kunci. Semua ronde tersebut adalah identik kecuali pada saat pemrosesan ronde terakhir dari tiap jenis kunci tersebut. Setiap ronde dari pemrosesan termasuk satu *byte* berdasarkan tahap substitusi, tahap *row-wise permutation*, tahap *column-wise mixing*, dan tambahan pada *round key*. Urutan dari empat tahap tersebut dieksekusi secara berbeda antara enkripsi dan dekripsi.

### *F. OpenWrt*

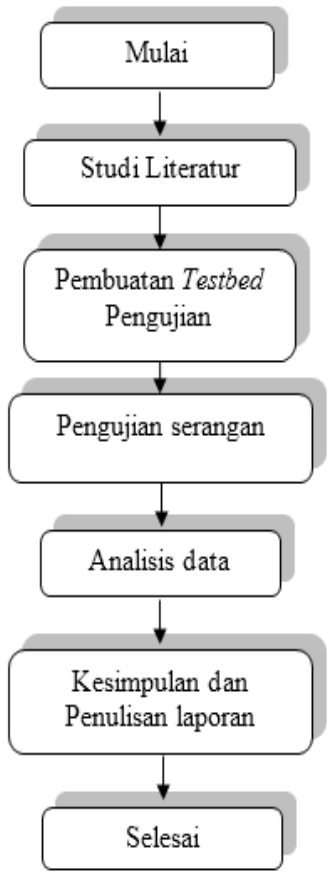
OpenWrt merupakan distribusi GNU/Linux yang dapat ditanamkan pada perangkat. OpenWRT adalah sistem operasi router yang dibangun untuk sebagai fungsi dasar router, memiliki fitur lengkap, dan mudah dimodifikasi. OpenWRT menyediakan *filesystem* yang dapat ditulis secara penuh (*fully writable*) dan disertai dengan manajemen paket. OpenWrt digunakan untuk memaksimalkan potensi yang dimiliki oleh suatu perangkat, terutama bagi perangkat yang lebih murah dan lama. OpenWRT memiliki banyak keuntungan diantaranya adalah [13]:

a. Kustomisasi dan kontrol penuh
b. Berbasis GPL, *Linux and Package Management.*
c. Menyediakan banyak fitur (lebih dari 3400 paket dan terus berkembang).
d. Secara aktif terus dikembangkan.
e. Dikembangkan menyeluruh ke perangkat berbiaya minim.

## III. METODOLOGI PENELITIAN

### *A. Tahapan Penelitian*

Tahapan-tahapan penelitian yang dilakukan adalah sebagai berikut:




Gambar 3 Tahapan penelitian

### *B. Kebutuhan Sistem*

Pada tahap ini dilakukan survei kebutuhan mengenai topik yang berkaitan dengan penelitian. Penulis mengumpulkan referensi dari survei dan penelitian terkait yang digunakan.

1) *Hardware:* Beberapa perangkat keras yang digunakan pada saat pengujian adalah:

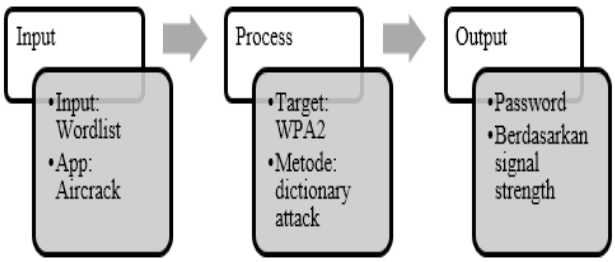
- Laptop dengan OS Kali Linux
- Laptop dengan OS Windows 7
- Router TP-Link 3040
- Modem Huawei K3765
- Kabel LAN

2) *Software:* Beberapa perangkat lunak yang digunakan pada saat pengujian adalah:

- OpenWrt
- Aircrack-ng
- inSSIDer
- Akismet

e-ISSN: 2252-7036
Vol.2 No.3 2017: 105-111

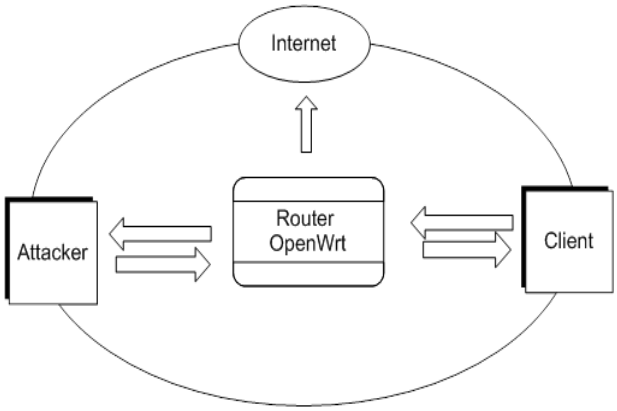
### C. *Prosedur Penelitian*




Gambar 4 Diagram Blok Penelitian

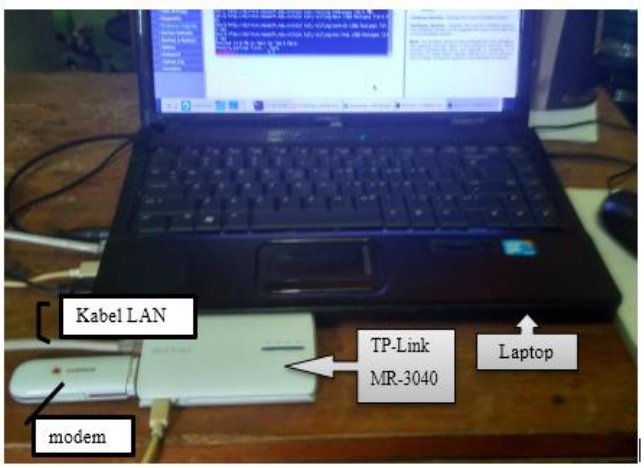
Diagram di atas menggambarkan proses pengujian dengan masukan berupa *wordlist*, proses dengan target pada WPA2 dengan metode *dictionary attack* dan keluaran berupa *password* dan waktu pengujian yang dicatat.

### D. *Konsep Perancangan Hardware*



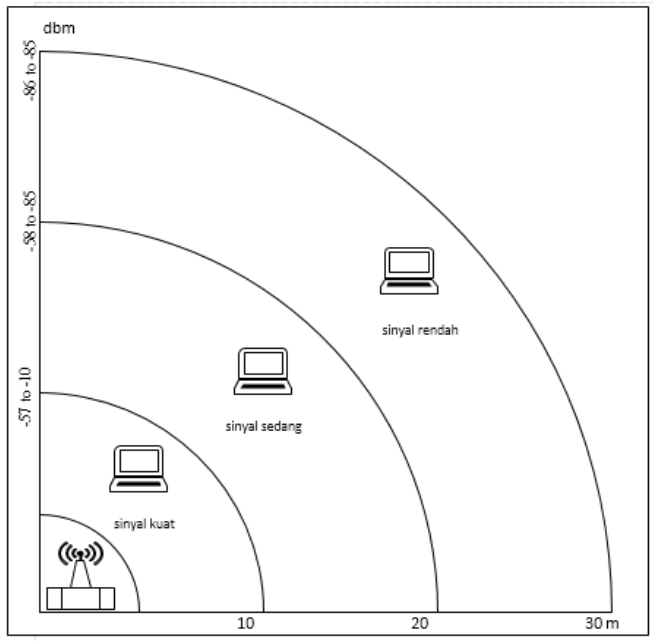

Gambar 5 Topologi jaringan penelitian

Pada gambar di atas menggambarkan bagaimana topologi penelitian, terdapat tiga hal utama yaitu *attacker* menggunakan *dictionary attack* untuk melakukan serangan pada *router* dan *client* yang terhubung pada *router* tersebut.




Gambar 6 Instalasi router, modem, dan kabel LAN

Gambar di atas menunjukkan sebuah *router* TP-Link 3040 terhubung ke modem, kabel LAN dan laptop. Pada *router* diinstal perangkat lunak OpenWrt untuk *routing* jaringan WiFi.



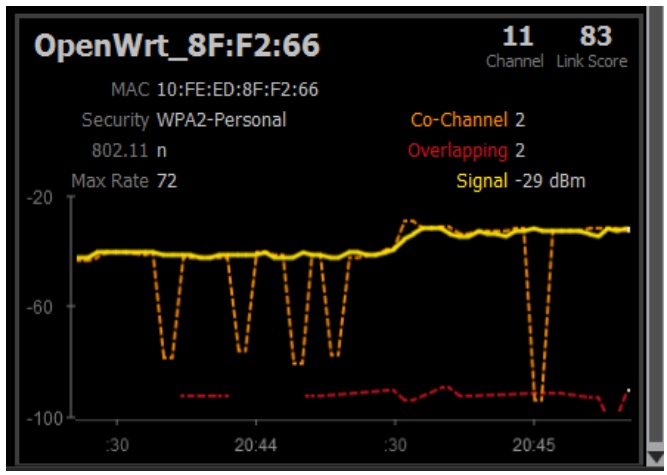

Gambar 7 Denah pengujian

Sesuai dengan denah pengujian dilakukan di dalam dan luar ruangan, dilakukan tiga kondisi pengujian masing-masing dengan *input password* yang berbeda. Pada kondisi pertama, diuji pada saat sinyal kuat, kedua pada saat sinyal sedang, dan ketiga pada saat sinyal rendah.

## IV. HASIL DAN PEMBAHASAN

### A. *Pengujian Signal Strength*

Sebelum dilakukan pengujian dan analisis hasil keamanan pada akses poin dengan keamanan WPA2, terlebih dahulu dilakukan *scanning* dengan inSSIDER atau *akismet* untuk melihat kekuatan sinyal yang akan diuji.




Gambar 8 Signal strength

e-ISSN: 2252-7036
Vol.2 No.3 2017: 105-111

Gambar di atas menunjukkan *access point* OpenWrt dengan *signal strength* bernilai -29 dBm, yang berarti termasuk dalam kategori *excellent*.

*B. Pengujian Signal Strength*

Tahapan yang dilakukan adalah sebagai berikut:

a. Mengaktifkan monitor WiFi dengan perintah *"airmon-ng start wlan0"*.
b. Pencarian terhadap AP dan client yang terhubung WiFi dengan *airodump-ng.*
c. Deautentikasi, untuk melakukan *capture handshake* dengan cara deautentikasi client yang terhubung WiFi. Untuk melakukan ini digunakan fitur *aireplay-ng*.
d. *Cracking*, dilakukan dengan *aircrack-ng*, dengan masukan berupa *wordlist.*

Data pengujian berupa *wordlist*, merupakan kumpulan kunci yang dijadikan masukan untuk dilakukan serangan dengan *dictionary attack*. Kata kunci tersebut dapat berupa huruf abjad maupun angka. Contoh *wordlist* yang dapat digunakan adalah:

TABEL II
WORDLIST

| ***Wordlist*** | |
|---|---|
| password | mickey |
| iloveyou | 1234567890 |
| 654321 | alexandra |
| 12345678superman | orange |
| fakultasteknikunsyiahftu | 789456 |
| universitassyiahkualausk | 999999 |

Gambar 9 berikut merupakan contoh hasil tangkapan gambar pada pengujian pertama.


Gambar 9 Hasil pengujian dengan aircrack-ng

Berikut ini adalah hasil pengujian-pengujian yang dilakukan pada saat kuat sinyal berbeda-beda yaitu pada saat sinyal kuat, sinyal sedang, dan sinyal rendah.

*1) Pengujian pada Signal Strength Kuat*: Pada pengujian pertama dilakukan pada saat kuat sinyal dengan rentang -57 dBm hingga -10 dBm (75% - 100%).

TABEL III
DATA PENGUJIAN PADA SINYAL KUAT

| ***No*** | ***Panjang*** | ***Posisi*** | ***Password*** | ***sinyal (dBm)*** | ***Waktu (s)*** |
|---|---|---|---|---|---|
| 1 | 8 | 4 | 12345678 | -39 | 00:37 |
| 2 | 8 | 51 | freewifi | -45 | 00:43 |
| 3 | 8 | 9 | password | -56 | 00:45 |
| 4 | 8 | 5 | iloveyou | -53 | 00:45 |
| 5 | 16 | 88 | 1234567890123456 | -50 | 00:40 |
| 6 | 16 | 135 | teknikelektrojte | -47 | 00:45 |
| 7 | 16 | 27 | password12345678 | -56 | 00:45 |
| 8 | 16 | 98 | 12345678superman | -56 | 00:45 |
| 9 | 24 | 15 | universitassyiahkualausk | -50 | 00:41 |
| 10 | 24 | 195 | fakultasteknikunsyiahftu | -47 | 00:41 |
| 11 | 24 | 151 | 123456781234567812345678 | -56 | 00:45 |
| 12 | 24 | 202 | ifyouknowwhatimeanwhynot | -57 | 00:46 |
| 13 | 32 | 75 | universitassyiahkualadibandaaceh | -51 | 00:45 |
| 14 | 32 | 207 | laporankemajuantugasakhirskripsi | -55 | 00:45 |
| 15 | 32 | 181 | wpawpa2openwrtrouteralternatives | -57 | 00:44 |
| 16 | 32 | 108 | pengujianparametersignalstrength | -56 | 00:46 |

Pada pengujian pertama dilakukan dengan kuat sinyal antara -39 dBm hingga -57 dBm. Berdasarkan hasil pengujian diketahui waktu yang tercepat 37 detik dan terlama 45 detik. Hasil menunjukkan bahwa password yang menggunakan angka "12345678" dengan *signal strength* -39 dBm terkuat merupakan yang paling cepat dibandingkan yang lainnya dengan hanya membutuhkan waktu 37 detik. Rata-rata waktu yang dibutuhkan pada saat pengujian serangan *dictionary attack* adalah 43,62 detik.

e-ISSN: 2252-7036
Vol.2 No.3 2017: 105-111

*2) Pengujian pada Signal Strength Sedang:* Pada pengujian kedua dilakukan pada saat kuat sinyal dengan rentang -75 dBm hingga -58 dBm (40% - 74%).

TABEL IV
DATA PENGUJIAN PADA SINYAL SEDANG

| *No* | *Panjang* | *Posisi* | *Password* | *Sinyal (dBm)* | *Waktu (s)* |
|---|---|---|---|---|---|
| 1 | 8 | 4 | 12345678 | -70 | 00:45 |
| 2 | 8 | 51 | freewifi | -65 | 00:46 |
| 3 | 8 | 9 | password | -58 | 00:45 |
| 4 | 8 | 5 | iloveyou | -58 | 00:45 |
| 5 | 16 | 88 | 1234567890123456 | -61 | 00:45 |
| 6 | 16 | 135 | teknikelektrojte | -67 | 00:44 |
| 7 | 16 | 27 | password12345678 | -58 | 00:45 |
| 8 | 16 | 98 | 12345678superman | -70 | 00:45 |
| 9 | 24 | 15 | universitassyiahkualausk | -73 | 00:44 |
| 10 | 24 | 195 | fakultasteknikunsyiahftu | -70 | 00:45 |
| 11 | 24 | 151 | 123456781234567812345678 | -75 | 00:46 |
| 12 | 24 | 202 | ifyouknowwhatimeanwhynot | -75 | 00:45 |
| 13 | 32 | 75 | universitassyiahkualadibandaaceh | -61 | 00:45 |
| 14 | 32 | 207 | laporankemajuantugasakhirskripsi | -68 | 00:46 |
| 15 | 32 | 181 | wpawpa2openwrtrouteralternatives | -71 | 00:46 |
| 16 | 32 | 108 | pengujianparametersignalstrength | -72 | 00:46 |

Pada pengujian kedua dilakukan dengan jarak 20 meter dengan kuat sinyal sedang berkisar antara -75 dBm hingga -58 dBm. Berdasarkan pengujian diketahui bahwa waktu yang diperlukan tercepat 44 detik dan terlama 46 detik. Rata-rata waktu yang dibutuhkan untuk melakukan proses serangan pada rentang sedang adalah 45,18 detik.

*3) Pengujian pada Signal Strength Rendah:* Pada pengujian ketiga dilakukan pada saat kuat sinyal dengan rentang -95 dBm hingga -86 dBm (0% - 19%).

TABEL V
DATA PENGUJIAN PADA SINYAL RENDAH

| *No* | *Panjang* | *Posisi* | *Password* | *sinyal (dBm)* | *Waktu (s)* |
|---|---|---|---|---|---|
| 1 | 8 | 4 | 12345678 | -87 | 00:45 |
| 2 | 8 | 51 | freewifi | -86 | 00:45 |
| 3 | 8 | 9 | password | -87 | 00:46 |
| 4 | 8 | 5 | iloveyou | -87 | 00:45 |
| 5 | 16 | 88 | 1234567890123456 | -86 | 00:46 |
| 6 | 16 | 135 | teknikelektrojte | -87 | 00:46 |
| 7 | 16 | 27 | password12345678 | -87 | 00:45 |
| 8 | 16 | 98 | 12345678superman | -88 | 00:45 |
| 9 | 24 | 15 | universitassyiahkualausk | -86 | 00:45 |
| 10 | 24 | 195 | fakultasteknikunsyiahftu | -87 | 00:45 |
| 11 | 24 | 151 | 123456781234567812345678 | -89 | 00:46 |
| 12 | 24 | 202 | ifyouknowwhatimeanwhynot | -88 | 00:45 |
| 13 | 32 | 75 | universitassyiahkualadibandaaceh | -87 | 00:47 |
| 14 | 32 | 207 | laporankemajuantugasakhirskripsi | -87 | 00:46 |
| 15 | 32 | 181 | wpawpa2openwrtrouteralternatives | -86 | 00:46 |
| 16 | 32 | 108 | pengujianparametersignalstrength | -88 | 00:45 |

Pada pengujian ketiga dilakukan dengan jarak lebih dari 30 meter dengan kuat sinyal lemah. Berdasarkan data hasil pengujian diketahui bahwa dengan sinyal antara -86 dBm hingga -89 dBm, diperlukan waktu mulai dari 45 detik hingga 47 detik. Pada pengujian ini, dengan sinyal -86 dBm dan *password* "universitassyiahkualadibandaaceh" merupakan waktu terlama terpaut dua detik dari yang tercepat. Rata-rata waktu yang dibutuhkan untuk melakukan proses *dictionary attack* pada rentang sinyal rendah ini adalah 45,5 detik.

*4) Pengujian berdasarkan Posisi Wordlist:* Pengujian ini dilakukan untuk mengetahui pengaruh posisi password pada wordlist pada saat pengujian menggunakan metode dictionary attack, dengan beberapa password sesuai dengan tabel 6 berikut.

e-ISSN: 2252-7036
Vol.2 No.3 2017: 105-111

TABEL VI
PENGUJIAN BERDASARKAN POSISI PASSWORD

| *No* | *Panjang* | *Posisi* | *Password* | *Sinyal (dBm)* | *Waktu (s)* |
|---|---|---|---|---|---|
| 1 | 8 | 80 | 12345678 | -70 | 00:45 |
| 2 | 16 | 80 | password12345678 | -80 | 00:45 |
| 3 | 24 | 80 | universitassyiahkualausk | -86 | 00:45 |
| 4 | 32 | 80 | universitassyiahkualadibandaaceh | -87 | 00:45 |

Berdasarkan tabel 6, dilakukan pengujian dengan menggunakan kombinasi karakter huruf dan angka berbeda dengan posisi *wordlist* yang sama menunjukkan hasil waktu yang sama untuk mendapatkan *password.*

## V. KESIMPULAN

Berdasarkan hasil pengujian dan penelitian yang dilakukan terhadap keamanan WPA2 dan pengaruh *signal strength* pada router berbasis OpenWrt, dapat disimpulkan bahwa keamanan WPA2 masih bisa ditembus oleh serangan *dictionary attack* selama *password* terdapat pada *wordlist*. Pengujian yang dilakukan pada tiga kondisi kuat sinyal, pada saat kuat sinyal tinggi, sedang, dan rendah mendapatkan waktu proses pengujian yang berbeda. Berdasarkan ketiga pengujian, diketahui bahwa kuat sinyal dengan satuan *dbm* berbeda hanya berpengaruh pada saat proses *cracking* (autentikasi, deautentikasi, *handshake capturing*), akan tetapi tidak berpengaruh terhadap berhasil atau tidaknya untuk mendapatkan password, hal tersebut dibuktikan dengan didapatkannya *password* yang terdapat pada *wordlist*.

## UCAPAN TERIMA KASIH

Secara khusus penulis mengucapkan terima kasih kepada Bapak Dr. Teuku Yuliar Arif, S.T., M.Kom selaku pembimbing I, dan Bapak Dr. Ir. Rizal Munadi, M.M., M.T selaku pembimbing II yang telah membimbing penulis dalam penulisan karya ilmiah ini.

## REFERENSI

[1] Mavridis, LP. Androulakis, A,-I, E, Halkias, A, B 2011, "Real-life paradigms of wireless network security attacks", vol.,no.,pp 1.
[2] Tiphon, 1999, "Telecommunications and Internet Protocol Harmonization Over Network (TIPHON) in General Aspects of Quality of Service (QoS)", DTR/TIPHON05006
[3] Slickkitten. 2013. "About OpenWRT". (http://wiki.openwrt.org/about/start, diakses 10 November 2016)
[4] Sya'ban, Dinisfu. "Routing". Sekolah Tinggi Sandi Negara Bogor, 2013.
[5] Shukla, Parth. "OpenWRT Introduction" in *Enterprise Security in Low Cost Hardware*.
[6] W. Purbo, Onno, "*Jaringan Wireless di Dunia Berkembang*", edisi kedua, Indonesia, 2007.
[7] Afdhal dan Elizar, "IEEE 802.11ac sebagai Standar Pertama", Jurnal Rekayasa Elektrika Vol. 11, Teknik Elektro FT Unsyiah, 2014, pp.3
[8] Wahana Komputer, "The Best Enryption Tools". Elex Media Komputindo, 2016.
[9] Bornhager, Malin. "Router and Routing", Halmstad University, 2012.
[10] A., Fikri, "Analisis dan Perbandingan Keamanan pada WLAN dengan Enkripsi AES dan TKIP", ITB, 2011.
[11] Finn Michael Halvorsen, Olav Haugen, "Cryptanalysis of IEEE 802.11i TKIP", Norwegian University of Science and Technology.
[12] Avi Kak, (2017), Lecture 8: AES: The Advanced Encryption Standard Lecture Notes on "Computer and Network Security", Avinash Kak, Purdue University.
[13] Shukla, Parth. "OpenWRT Introduction" in *Enterprise Security in Low Cost Hardware*.
[14] Jin, Tao. "OpenWrt Development Guide", Februari 2012.
[15] Industri, Veris. 2013. "Veris Aerospond Wireless Sensors Received Signal Strength Indicator (RSSI)".