PENGUJIAN PERFORMANSI KEAMANAN *WIRELESS LAN* MENGGUNAKAN *WIRELESS INTRUSION DETECTION SYSTEM*

SECURITY PERFORMANCE TESTING OF WIRELESS LAN USING WIRELESS INTRUSION DETECTION SYSTEM

Iqbal Firda Rusdiansyah[1], Sofia Naning Hertiana, S.T., M.T.[2], Ridha Muldina Negara, S.T., M.T.[3]
[1,2,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
[1]**iqbalfr@students.telkomuniversity.ac.id**, [2]**sofiananing@telkomuniversity.co.id**,
[3]**ridhanegara@telkomuniversity.ac.id**

Abstrak

Perkembangan jaringan internet yang semakin pesat dan besar mendorong peningkatan penggunaan jaringan *Wireless Local Area Network* (WLAN) sebagai *gateway* bagi *endpoint device* untuk mengakses jaringan internet. WLAN memiliki kelebihan yakni memiliki kecepatan transfer data tinggi, praktis digunakan, dan fleksibel karena menggunakan media transmisi gelombang radio untuk terhubung dengan user. Namun karena transmisi paket dilakukan secara terbuka membuat jaringan WLAN lebih rentan terhadap pencurian data dan serangan *cybers*.

Untuk mengamankan jaringan WLAN terdapat sistem keamanan yang sudah mumpuni yakni *Wireless Intrusion detection system* (WIDS). WIDS memiliki prinsip yang sama dengan IDS namun dikhususkan untuk melindungi jaringan WLAN dari serangan. Sehingga WIDS cocok dipasangkan pada jaringan WLAN karena dapat mendeteksi serangan di udara sehingga admin jaringan dapat melakukan tindakan sebelum serangan merusak komponen penting yakni *server*, *access point,* dan *client.*

Dalam tugas akhir ini, sistem keamanan WIDS akan dipasangkan pada jaringan WLAN yang dijalankan menggunakan *emulator* Mininet-Wifi. Sistem yang telah dibuat diuji menggunakan serangan yang khusus ditujukan untuk jaringan WLAN (WEP, WPA, WPA2 *Cracking*; *Denial of Service*; dan *Evil-Twin*) dan diuji performansi QoS-nya saat sebelum dan setelah dipasang WIDS dan saat dijalankan dengan trafik video dan VoIP dengan *bacgkround traffic* 10 Mbps hingga 58 Mbps. Hasilnya sistem dapat mendeteksi serangan WEP, WPA, dan WPA2 *Cracking*; dan *Denial of Service* namun tidak dapat menentukan sumber serangan dengan tepat (*false positive*). Untuk serangan *Evil-Twin* dapat dideteksi dengan baik oleh sistem. Dari uji performansi, didapat hasil pemasangan WIDS hanya berpengaruh terhadap kenaikan *delay* rata-rata. Begitu juga dengan kondisi *background traffic* yang berbeda hanya terjadi peningkatan secara linear pada *delay* rata-rata. Untuk *jitter throughput,* dan *packet loss* cenderung stabil dari hasil dua uji performansi yang dilakukan.

Kata Kunci : WLAN, WIDS, *access point.*

Abstract

The development of increasingly fast and large internet networks has encouraged an increase in the use of Wireless Local Area Network (WLAN) networks as a gateway for device endpoints to access internet networks. WLAN has the advantage of having high data transfer speeds, practical use, and flexibility because it uses radio wave transmission media to connect with users. However, because packet transmission is carried out openly, making WLAN networks more vulnerable to data theft and attack by cybers.

To secure the WLAN network, there is a security system that is qualified, namely the Wireless Intrusion detection system (WIDS). WIDS has the same principles as IDS but is specifically intended to protect WLAN networks from attacks. So that WIDS is suitable to be installed on a WLAN network because it can detect attacks in the air so the network admin can take action before the attack damages important components, namely the server, access point, and client.

In this final project, the WIDS security system will be installed on a WLAN network that is run using the Mininet-Wifi emulator. Systems that have been made are tested using attacks specifically intended for WLAN networks (WEP, WPA, WPA2 Cracking; Denial of Service; and Evil-Twin) and QoS performance is tested before and after WIDS is installed and when run with video and VoIP traffic with backround traffic of 10 Mbps to 58 Mbps. The result is that the system

can detect WEP, WPA, and WPA2 Cracking attacks; and Denial of Service but cannot determine the source of the attack correctly (false positive). Evil-Twin attacks can be detected properly by the system. From the performance test, it was found that the WIDS installation results only affected the increase in average delay. Likewise, with different background traffic conditions there is only a linear increase in average delay. For jitter throughput, and packet loss tend to be stable from the results of two performance tests performed.
Keywords : WLAN, WIDS, access point.

1. Pendahuluan

Seiring berjalannya waktu, perkembangan jaringan internet semakin meningkat pesat seiring meningkatnya jumlah user dan endpoint device yang membutuhkan layanan internet [1]. Hal ini menyebabkan meningkatnya jumlah perangkat gateway sebagai pintu masuk untuk mengakses jaringan internet. Tak terkecuali gateway pada jaringan WLAN yang menggunakan *Access point* (AP). Jaringan WLAN menjadi jaringan yang banyak digunakan untuk terhubung dengan layanan internet baik secara privat maupun public [2]. Hal ini dikarenakan jaringan WLAN menggunakan gelombang radio untuk mentransmisikan data sehingga kecepatan transfer data cepat, praktis digunakan tanpa harus terhubung dengan kabel, dan fleksibel digunakan dalam posisi apapun selama *client* masih berada dalam cakupan gelombang radio dari AP. Namun karena transfer data yang bersifat terbuka menyebabkan data-data yang dikirimkan dalam proses transmisi dapat di¬-capture oleh siapapun sehingga jaringan WLAN sangat rentan terhadap pencurian data dan serangan *cyber*.

Serangan *cyber* pada jaringan WLAN yang sering terjadi berasal dari *client* atau endpoint device dalam cakupan gelombang radio AP. Biasanya penyerang melakukan monitoring terhadap paket-paket yang beredar pada gelombang radio AP untuk mencari informasi dan titik lemah dari AP untuk melakukan serangan terhadap jaringan ataupun *client* lain yang terhubung. Meskipun kini jaringan WLAN kebanyakan sudah memiliki sistem enkripsi yang mengubah paket data yang beredar pada gelombang radio AP menjadi cypher text dan mengharuskan *client* melakukan otentikasi *password* terlebih dahulu dengan AP. Serangan tidak dapat dihindarkan apabila penyerang memiliki *password* tersebut dan sistem enkripsi tersebut jarang digunakan pada jaringan WLAN publik. Sehingga untuk melindungi jaringan WLAN ini diperlukan sistem keamanan yang bisa mendeteksi serangan di titik AP yang berasal dari *client* sah maupun perangkat lain yang bukan *client*. Sistem keamanan yang cocok adalah *Wireless Intrusion Detection System* (WIDS). WIDS adalah sistem keamanan WLAN yang dapat mendeteksi serangan-serangan yang dilancarkan dalam secara *wireless*. WIDS dapat dipasang dalam sensor terpisah dari AP atau dapat dijalankan dalam satu perangkat AP yang sama (hanya untuk perangkat yang mendukung).

Dalam tugas akhir ini, sistem keamanan WIDS dipasangkan pada jaringan WLAN yang dijalankan menggunakan emulator Mininet-Wifi. WIDS yang akan digunakan adalah WAIDPS (*Wireless* Auditing and IPS/IDS), yakni WIDS *open source* yang juga dapat digunakan untuk menguji serangan terhadap jaringan WLAN. Sistem jaringan ini diuji dengan serangan yang khusus ditujukan bagi jaringan WLAN untuk mengetahui kelayakan WIDS dalam mendeteksi serangan dan untuk mengetahui pengaruh pemasangan WIDS terhadap performa jaringan..

2. Dasar Teori

2.1 *Wireless* Local Area Network (WLAN)

WLAN menghubungkan dua atau lebih *device* dengan menggunakan metode distribusi (pada umumnya menggunakan *spread-spectrum* atau OFDM) dan biasanya memberikan sebuah koneksi ke jaringan Internet kabel melalui sebuah AP (*Access Point*). Memberikan kemudahan bagi user untuk melakukan mobilitas pada daerah cakupan lokal dan tetap terkoneksi ke jaringan. Kebanyakan WLAN yang modern merujuk ke sebuah standar yaitu IEEE 802.11, dan di pasarkan dalam nama Wi-Fi [3].

Sebuah WLAN terdiri atas sebuah *node* dan AP. Sebuah *node* tersebut adalah computer atau *periferal* seperti *printer* yang memiliki sebuah adapter jaringan, misalnya sebuah antena. AP berfungsi sebagai *transmitter* dan *receiver* antara *node* atau antara *node* pada jaringan yang berbeda. *Wireless Fidelity* atau Wi-Fi adalah jenis mekanisme jaringan *Wireless* (IEEE 802.11) sebagai produk dari Wi-Fi *Alliance* yang sering digunakan pada industri. Jaringan ini digunakan pada tempat-tempat umum seperti tempat perbelanjaan, restoran, perpustakaan, kampus, sekolah dan tempat-tempat umum lainnya.

2.2 *Wireless Intrusion detection system*

Secara umum, *Instrusion Detection System* (IDS) didesain dan dibuat untuk memonitor dan melaporkan aktivitas yang berlangsung dalam jaringan kepada *administrator*. WIDS membutuhkan sensor untuk mengumpulkan data data dalam jaringan, *server* untuk mengolah data-data yang telah dikumpukan, dan *client* untuk menampilkan hasil dari pengolahan data yang telah dikumpulkan. *Interface* WIDS ditempatkan pada *client* WIDS.

WIDS dapat mendeteksi serangan pada *frame* 802.11 pada layer dua dari jaringan *wireless*. Ada tiga tipe *frame* MAC 802.11, yaitu *frame* data, kontrol, dan manajemen. Mayoritas serangan *wireless* menjadikan *frame* manajemen sebagai targetnya karena *frame* ini bertugas untuk melakukan autentikasi, asosiasi, disasosiasi, *beacon*, dan *Probe request/Response*. Serangan *wireless* seperti *Man-in-the-Middle* (MITM), *rogue* AP, *war driver*, dan *denial-of-service* berjalan pada *frame* 802.11 dan tidak bisa dideteksi pada layer tiga. IDS biasa (pada jaringan kabel) tidak dapat menerima *frame* ini, karena *frame* manajemen tidak dapat diteruskan ke layer di atasnya.

WIDS membutuhkan *interface* khusus. *Interface wireless* ini harus dioperasikan pada mode monitor, yang dikenal juga sebagai mode RFMON. Mode ini membolehkan *device* untuk menerima semua lalu lintas yang masuk. *Interface* yang bertugas memonitor harus terus berganti *channel*, dikenal dengan *channel hopping*, yang tersedia pada jaringan tersebut. Beberapa serangan *wireless* bekerja dengan menggunakan *rogue* AP pada *channel* yang berbeda. Sebagai contoh, serangan MIM menggunakan *rogue* AP yang paling sedikit berbeda lima *channel* dari *target* AP. Tanpa *channel* hopping, WIDS dapat luput terhadap serangan yang dilakukan pada *channel* lain. Walaupun begitu, deteksi ini hanya dapat berjalan pada jaringan *wireless* dengan satu AP saja, karena jaringan yang lebih besar akan mempunyai beberapa AP yang dikonfigurasi pada *channel* yang berbeda untuk menghindari interferensi frekuensi radio dengan AP yang lain.

Untuk mendeteksi serangan pada *range* tertentu, WIDS mencocokkan serangan dengan metodologi deteksi *signature-based*, *knowledge-based*, dan analisis protokol *stateful*. Deteksi *signature-based* menggunakan *signature static* untuk mencocokkan lalu lintas yang mencurigakan. Tipe pencocokan ini bekerja dengan baik untuk serangan-serangan yang telah dikenal sebelumnya dan cocok dengan pola tertentu. Sebagai contoh, untuk mendeteksi *rogue* AP, WIDS menggunakan daftar AP yang sah dan memberikan sinyal jika ada AP yang terdeteksi tidak cocok dengan daftar. Deteksi knowledge-based menggunakan acuan dasar historis dan memberikan sinyal ketika lalu lintas jaringan berbeda dari acuan dasar historis. Beberapa serangan *wireless* tidak cocok dengan signature tetapi serangan ini dapat menyebabkan anomali lalu lintas jaringan.

Analisis protokol stateful merupakan proses membandingkan profil yang sudah ditentukan sebelumnya. Analisis protokol *stateful* bergantung pada profil yang dikembangkan vendor secara *universal* yang menspesifikasikan bagaimana protokol tertentu seharusnya digunakan. Kata "stateful" berarti IDS mampu memahami dan mengikuti keadaan protokol *network*, *transport*, dan *application*. Sebagai contoh, ketika user memulai sesi *File Transfer Protocol* (FTP), sesi pertama-tama berada pada keadaan yang belum sah. User yang tidak sah seharusnya hanya dapat melakukan perintah-perintah tertentu pada keadaan ini, seperti melihat informasi bantuan. Bagian penting memahami keadaan adalah mencocokkan *request* dengan *Response*, jadi ketika autentikasi FTP terjadi, IDS dapat menentukan apakah sukses atau tidak dalam menemukan kode status dalam respon yang sesuai. Ketika *user* sudah berhasil diautentikasi, sesi ada pada keadaan sah, dan *user* dapat melakukan beberapa perintah lainnya. Melakukan hampir semua perintah ketika masih dalam keadaan tidak sah dapat dipertimbangkan sebagai keadaan yang mencurigakan

3. Pembahasan

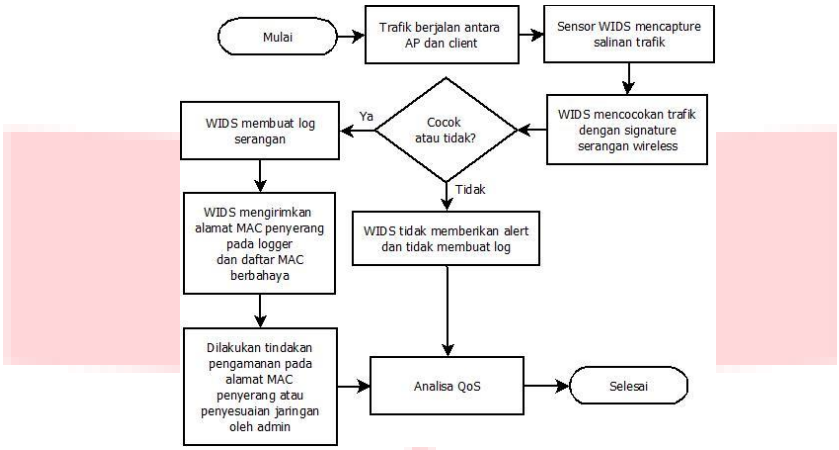
3.1. Gambaran Umum

Sistem Sistem yang dibuat adalah jaringan WLAN yang dihubungkan dengan sebuah sistem keamanan WIDS yang memonitor trafik menggunakan sensor dan memberikan alert pada *logger* ketika serangan terjadi pada daerah gelombang radio AP. Sistem yang dibuat dijalankan secara hybrid antara lingkungan *virtual* dan *physical*. Komponen switch berada dalam lingkup *virtual*. Empat perangkat Wifi (1 untuk AP, 2 untuk alat penyerang, 1 untuk sensor WIDS dan) dan dua *client* (sebagai *client* normal dan *attacker*) berada dalam lingkup *physical*. Sementara sistem WIDS berada diantara lingkup *virtual* dan *physical*.

Sistem selanjutnya diuji keamanannya pada titik daerah gelombang radio AP yang ada di lingkup *physical*. Pengujian keamanan dilakukan menggunakan serangan-serangan yang biasa ditujukan pada jaringan WLAN secara *wireless*. Serangan-serangan tersebut ditujukan pada AP dan/atau *client*. Setelah serangan dilancarkan, sistem keamanan WIDS diuji apakah dapat mendeteksi dan memberi alert pada *logger*. Selain itu sistem WIDS juga diuji terhadap trafik normal

apakah sistem dapat melakukan kesalahan dengan mendeteksi trafik normal sebagai kesalahan. Selanjutnya sistem jaringan diukur secara QoS untuk mengetahui kelayakan performa jaringan setelah dipasangkan dengan sistem keamanan WIDS. Parameter yang diukur dalam uji QoS adalah latency, *jitter*, *packet loss*, dan *throughput*.

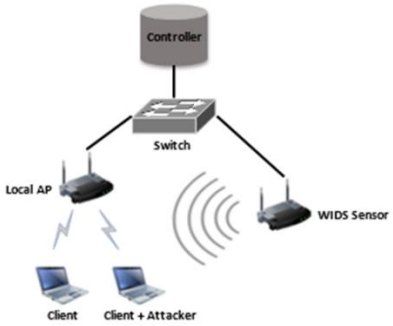
3.1.1. Alur Kerja Sistem



Gambar 3.1 Diagram Alir

3.1.2. Rancangan Topologi Sistem

Topologi jaringan yang dibangun dalam jaringan WLAN ini adalah sebagai berikut:



Gambar 3.2 Topologi Jaringan

3.1. Desain Perangkat Keras

Tabel 3.1 Spesifikasi *hardware* yang digunakan

Spesifikasi	Perangkat		
	Laptop 1	**Laptop 2**	**Phone 3**
Processor	Intel Core i5	Intel Celeron Dual Core	Qualcomm Snapdragon
RAM	4 GB	2 GB	2 GB
Hardisk	1 TB	500 GB	16 GB
Peran	Mininet-Wifi *emulator* dan WAIDPS	*attacker* & *client*	*Client*

3.3. Desain Perangkat Lunak

Perangkat lunak yang digunakan dalam penelitian ini adalah sebagai berikut:

1.Mininet-WiFi sebagai emulator jaringan.
2.WAIDPS sebagai keamanan WIDS.
3.OS Ubuntu sebagai OS pada laptop selain laptop *attacker*.
4.Kali Linux sebagai OS laptop *attacker*.

5.Aircrack-NG Suite sebagai alat penyerang yang diinstal dalam Kali Linux.
6.Android 9.0 sebagai OS smartphone *client*.

3.4. Skenario Pengujian Sistem

Pengujian Sistem jaringan WLAN dibagi menjadi dua jenis pengujian. Pengujian pertama yang dilakukan adalah uji serangan yang bertujuan menguji apakah WIDS yang dipasangkan pada jaringan dapat mendeteksi serangan yang umumnya dilancarkan pada jaringan *wireless*. Pengujian kedua adalah uji performansi untuk mengukur kelayakan sistem jaringan yang dibuat sesuai standar ITU-T G.1010.

3.4.1 Skenario Uji Serangan

Uji serangan yang dilakukan dalam penelitian ini meliputi 3 jenis serangan yaitu WEP, WPA, WPA2 cracking; Denial of Service (DoS) attack; dan Evil Twin.

3.4.2 Skenario Uji Performansi

Uji performansi meliputi pengukuran QoS sebelum dan setelah sensor WIDS dipasangkan pada sistem yang bertujuan mengukur pengaruh dipasangnya sensor terhadap QoS; dan pengukuran QoS pada kondisi *background traffic* sebesar 10 Mbps, 20 Mbps, 30 Mbps, 40 Mbps, kemudian 50 Mbps dinaikkan 1 Mbps secara bertahap hingga 60 Mbps, untuk mengetahui pada titik mana terjadi perubahan performansi jaringan secara signifikan. Parameter QoS yang digunakan adalah *latency*, *jitter*, *packet loss*, dan *throughput*.

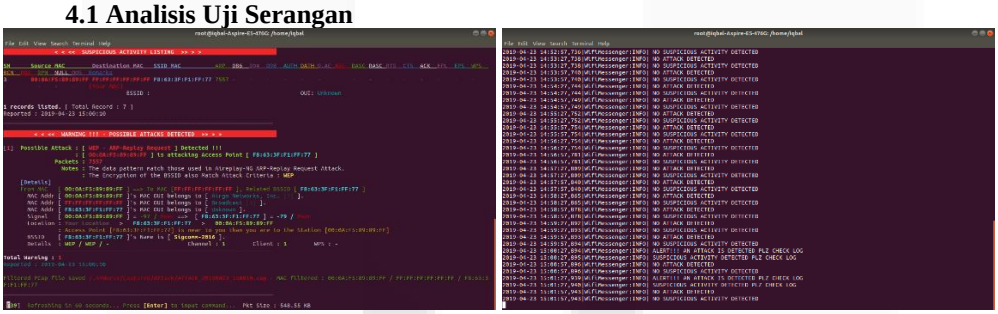
Pengujian pertama dilakukan dengan mengirimkan trafik UDP berjenis pket data 100 paket per detik dengan ukuran paket yang menggunakan distribusi poisson $\mu = 48$ bytes.

Pengujian kedua dilakukan dengan mengirimkan dua jenis trafik UDP yang dibangkitkan menggunakan packet generator D-ITG. Trafik yang dibangkitkan antara lain:

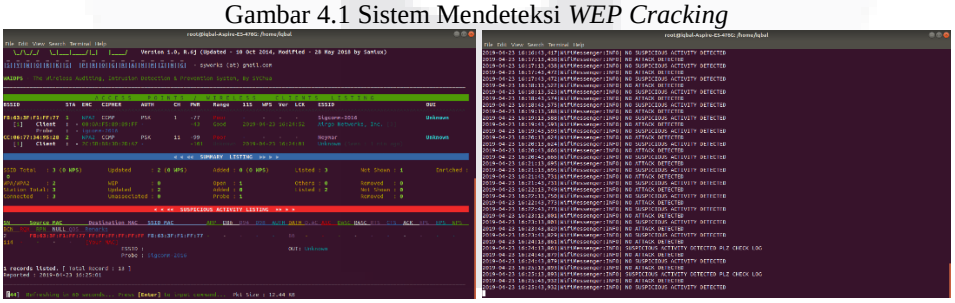
1. Video streaming 24 *frame* per detik, yang mana satu *frame* sama dengan satu paket yang menggunakan distribusi normal $\mu = 27791$ bytes dan $\sigma 2 = 6254$ bytes.
2. VoIP menggunakan codec G.711 sebanyak 100 paket per detik, ukuran paket 80 bytes, tanpa menggunakan Voice Activation Detection (VAD).

4. Pengujian dan Analisis Implementasi Sistem

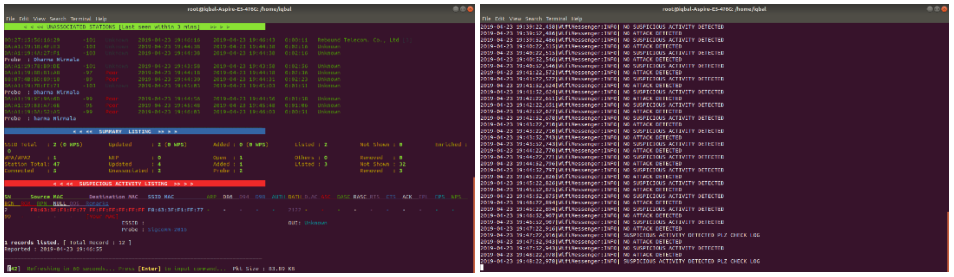
4.1 Analisis Uji Serangan



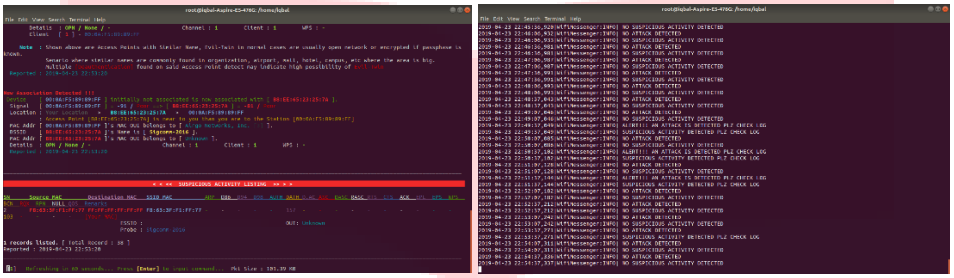
Gambar 4.1 Sistem Mendeteksi *WEP Cracking*



Gambar 4.2 Sistem Mendeteksi *WPA/WPA2 Cracking*



Gambar 4.3 Sistem Mendeteksi DoS

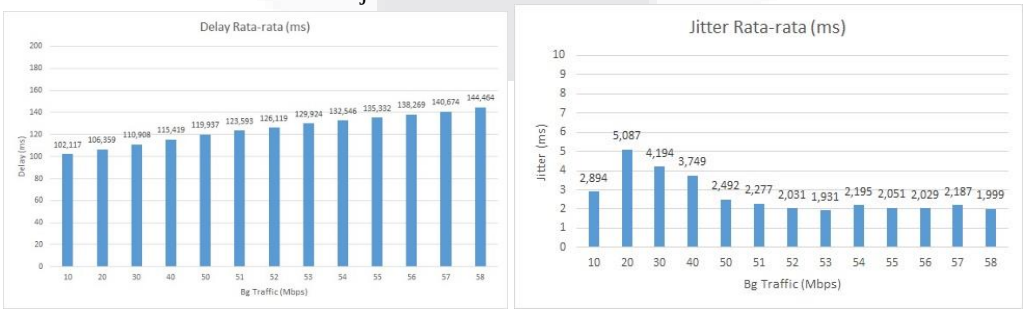


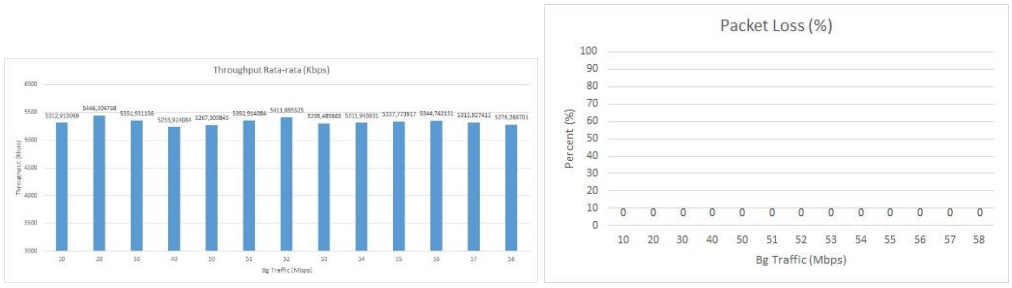
Gambar 4.4 Sistem Mendeteksi *Evil Twin*

Software WAIDPS yang digunakan dapat mendeteksi serangan WEP *cracking* dengan baik, namun terjadi *false positive* saat mendeteksi WPA/WPA2 *cracking*, DoS, dan *evil twin*. *False positive* yang terjadi adalah *alert* serangan tidak muncul namun hanya *alert* aktivitas mencurigakan yang terjadi, hal ini dikarenakan WAIDPS tidak dapat menentukan darimana asal paket serangan karena penyerang memodifikasi sumber serangan menjadi alamat perangkat yang legal.

4.1 Analisis Uji Performansi

Gambar 4.5 Hasil Uji Performansi Sebelum dan Setelah Performansi





Gambar 4.6 Hasil Uji Performansi Trafik Video

Gambar 4.7 Hasil Uji Performansi Trafik VoIP

5. Kesimpulan

Hasil analisis system memberikan kesimpulan sebagai berikut:

1. Software WAIDPS yang digunakan dapat mendeteksi serangan WEP *cracking* dengan baik, namun terjadi *false positive* saat mendeteksi WPA/WPA2 *cracking*, DoS, dan *evil twin*. *False positive* yang terjadi adalah *alert* serangan tidak muncul namun hanya *alert* aktivitas mencurigakan yang terjadi, hal ini dikarenakan WAIDPS tidak dapat menentukan darimana asal paket serangan karena penyerang memodifikasi sumber serangan menjadi alamat perangkat yang legal.
2. Meski terdapat bug/error, integrasi antara WAIDPS dan *logger* berjalan dengan baik karena *alert* muncul di waktu yang sesuai, sehingga admin dapat melakukan tindakan dengan segera. Selain itu WAIDPS juga menyimpan data riwayat serangan dan aktivitas mencurigakan dengan tepat. Sehingga WAIDPS masih layak untuk dipasangkan pada jaringan WLAN.
3. Pemasangan WAIDPS pada jaringan WLAN hanya mempengaruhi besar *delay* trafik data terhadap jaringan. *Delay* terhadap jaringan naik sebanyak 77 ms dari 30 ms ke 107 ms. Hal ini disebabkan WAIDPS beroperasi pada *channel* yang sama dengan AP fisik. Angka tersebut tergolong layak karena di bawah nilai *delay* maksimum 200 ms (ITU-T G.1010).
4. Nilai *jitter*, *throughput*, dan *packet loss* trafik data tidak dipengaruhi pemasangan WAIDPS karena nilainya cenderung tetap antara sebelum dan setelah pemasangan WAIDPS (berturut-turut nilainya 0,04 ms, 38 kb/s, dan 0%).
5. Pengaruh peningkatan *background traffic* berbanding lurus dengan peningkatan *delay* rata-rata trafik video dan VoIP dan masih memenuhi kelayakan (< 200 ms untuk video;<150 ms untuk VoIP). Sementara *jitter* rata-rata, *throughput* rata-rata, dan *packet loss* trafik video dan VoIP tidak dipengaruhi oleh *background traffic*. Besar *jitter* rata-rata stabil di angka ±2 ms untuk trafik video dan VoIP; Besar *throughput* rata-rata untuk trafik video stabil di 5,2 Mbps – 5,5

Mbps sementara trafik VoIP stabil di 73 Kbps; dan *packet loss* tidak terjadi pada trafik video dan trafik VoIP.

6. Perangkat *Access point* dapat membatasi *bandwidth* yang digunakan *background traffic* sehingga tidak tejadi penurunan *throughput* rata-rata trafik video dan trafik VoIP.
7. *Packet loss* tidak terjadi di pengujian performansi karena pengujian dilakukan di tempat yang tidak terdapat banyak perangkat *wireless*. Selain itu perangkat yang diujikan berdekatan satu sama lain sehingga besar daya sinyal yang dikirimkan perangkat besar. Hal ini dikarenakan keterbatasan tempat dan jumlah perangkat yang dapat digunakan untuk pengujian.

Daftar Pustaka:

[1] Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021", 2017, www.cisco.com.
[2] Al Shourbaji, Ibrahim, "An Overview of *Wireless* Local Area Networks", 2013
[3] Dr. S. Dhanalakshmi, M. Sathiya, "An Overview of IEEE802.11 *Wireless* LAN Technologies", IJCSMC, Vol. 4, Issue. 1, January 2015, pg.85 – 93.
[4] I. Bartolic, "How WLAN Works", 2017, thebest*wireless*internet.com
[5] Gast, Matthew, "802.11® *Wireless* Networks: The Definitive Guide", April 2002, California : O'Reilly.
[6] S. Gill, Rupinder, "Intrusion Detection Techniques in *Wireless* Local Area Networks", Dissertation, Bachelor of Information Technology Honours (Software Engineering and Data Communication), Queensland University of Technology, 2002.
[7] Fontes, Ramon & Afzal, Samira & H. B. Brito, Samuel & Santos, Mateus & Esteve Rothenberg, Christian, "Mininet-WiFi: Emulating software-defined *wireless* networks", 2015, 10.1109/CNSM.2015.7367387.
[8] International Telecomunication Union, "Series G: Transmission Systems and Media, Digital Systems and Networks, Quality Of Service and Performance, End-user multimedia QoS categories", ITU-T Recommendation G.1010, 2011.