SKANIKA: Sistem Komputer dan Teknik Informatika
Volume 8, Nomor 1, Januari 2025, Halaman 35-45 E-ISSN: 2721-4788

Evaluasi Dampak Opportunistic Wireless Encryption (OWE) Terhadap Kinerja Jaringan Nirkabel IEEE 802.11ax

Vian Ardiyansyah Saputro[1*], Ariep Jaenul[2]
[1]Politeknik Astra, Manajemen Informatika, Bekasi, Indonesia
[2]Magister Teknik Elektro, Universitas Global Jakarta, Depok, Indonesia
E-mail: [1*]vian.saputro@polytechnic.astra.ac.id, [2]ariep@jgu.ac.id
(* : corresponding author)

Abstrak

Masalah keamanan merupakan hal yang menjadi perhatian saat menggunakan jaringan nirkabel, terutama dalam situasi di mana jaringan terbuka digunakan. Opportunistic Wireless Encryption (OWE) dapat menjadi solusi memperbaiki perlindungan pada jaringan nirkabel yang terbuka selain menggunakan perlindungan yang terenkrispi. Penelitian ini bertujuan untuk mengukur dampak penggunaan implementasi OWE di jaringan 802.11ax terhadap metrik kinerja jaringan nirkabel seperti throughput dan packet loss dibandingkan dengan penggunaan open security melalui pendekatan eksperimental dalam topologi client server, pengujian mencakup pengukuran throughput maksimum menggunakan protokol TCP dengan ukuran paket 384 KB, 640 KB, dan 1408 KB, serta pengukuran packet loss menggunakan protokol UDP dengan ukuran data 10 MB, 100 MB, dan 1000 MB. Hasil yang didapatkan menunjukan bahwa ketika jaringan nirkabel menggunakan OWE mengalami penurunan performa seiring dengan peningkatan ukuran paket. Penurunan ini menunjukkan bahwa overhead enkripsi pada OWE dapat mempengaruhi kinerja, terutama pada ukuran paket yang besar. penurunan metrik throughput saat menggunakan OWE memiliki selisih 5 hingga 10 Mbps bila dibandingkan dengan penggunaan open security, sedangkan pada metrik packet loss kehilangan paket data terbesar saat menggunakan bandwidth 100 MB yaitu sebesar 16%. Temuan ini mengindikasikan bahwa meskipun OWE meningkatkan keamanan pada jaringan terbuka, overhead enkripsi dapat mempengaruhi kinerja.

Kata kunci: IEEE 802.1ax, Opportunistic Wireless Encryption, throughput, packet loss.

Abstract

Security is a critical concern when using wireless networks, especially on open networks. Opportunistic Wireless Encryption (OWE) provides a solution to enhance protection on open wireless networks through encryption. This study evaluates the impact of OWE implementation on the performance of 802.11ax networks, focusing on metrics such as throughput and packet loss, compared to open security. An experimental approach was conducted in a client-server topology, measuring maximum throughput using the TCP protocol with packet sizes of 384 KB, 640 KB, and 1408 KB. Packet loss was also measured using the UDP protocol with data sizes of 10 MB, 100 MB, and 1000 MB. The results indicate that using OWE leads to performance degradation as packet size increases. Throughput decreases by 5–10 Mbps compared to open security, while the highest packet loss of 16% occurs with a bandwidth of 100 MB. These findings highlight that the encryption overhead in OWE affects performance, particularly with larger packet sizes. Despite the performance impact, OWE significantly enhances the security of open networks. However, the trade-off between performance and security should be carefully considered when implementing OWE in practical scenarios.

***Keywords**: IEEE 802.1ax, Opportunistic Wireless Encryption, throughput, packet loss.*

1. PENDAHULUAN

Perkembangan jaringan nirkabel telah membuka akses komunikasi data yang cepat dan praktis bagi masyarakat luas untuk menunjang penggunaan di lingkungan kerja maupun sosial. Dengan adanya jaringan nirkabel memberikan kemudahan diantaranya fleksibel dalam penggunaannya [1]. Di antara berbagai standar jaringan nirkabel, standar jaringan nirkabel generasi terbaru yang dikenal sebagai Wi-Fi 6, adalah salah satu teknologi terkini yang menawarkan kapasitas jaringan dengan meningkatnya kecepatan dan stabilitas yang didapatkan pengguna [2]. Wi-Fi 6 dirancang untuk memenuhi tuntutan jaringan di lingkungan yang padat pengguna dan mengoptimalkan komunikasi data dalam situasi yang memerlukan *throughput*

tinggi dan latensi rendah [3]. Namun, di balik peningkatan kinerja ini, masih ada tantangan dalam memastikan keamanan dan privasi data pengguna dari penggunaan akses yang tidak sah atau yang biasa kita kenal sebagai keamanan jaringan [4]. Hal ini menjadi perhatian utama karena pada dasarnya sistem yang tidak aman dapat menjadi celah yang digunakan oleh hacker maupun cracker [5].

Masalah keamanan merupakan hal yang menjadi perhatian saat menggunakan jaringan nirkabel, terutama dalam situasi di mana jaringan terbuka digunakan. Jaringan terbuka, yang umumnya tidak menggunakan kata sandi untuk otentikasi, rentan terhadap risiko serangan untuk mengakses data pengguna yang tidak terenkripsi [6], seperti *man-in-the-middle*, penyadapan data [7], pembobolan username dan password [8]. Meskipun jaringan Wi-Fi yang aman biasanya menggunakan *wireless security protocol*.

Berkenaan dengan adanya celah keamanan pada jaringan nirkabel seperti yang telah disebutkan, untuk memperkuat keamanan jaringan nirkabel, salah satu solusi yang dapat diterapkan adalah dengan mengaktifkan protokol keamanan nirkabel seperti WPA, WPA2 [9] maupun WPA3 [10] di perangkat *access point* yang digunakan, namun cara ini dapat menyebabkan menurunnya kualitas *throughput* yang didapatkan oleh pengguna jaringan nirkabel [11].

Studi yang telah dilakukan untuk membandingkan tiga *wireless security protocol* yaitu *No security*, WPA versi 2 dengan enkripsi AES dan WPA versi 3 dengan enkripsi SAE pada jaringan *wireless* 802.11ax, hasilnya menunjukan bahwa pada *channel* 20 Mhz *throughput* mengalami penurunan sebesar 0.9% baik saat menggunakan WPA2-AES dan WPA3-SAE, dan untuk *channe*l 40 Mhz penggunaan WPA2-AES *throughput* mengalami penurunan sebesar 1.79%, sedangkan untuk *channel* 80 Mhz penggunaan WPA2-AES *throughput* mengalami penurunan sebesar 1.48% dan untuk WPA3-SAE sebesar 9.50% [11].

Selanjutnya pada penelitian lain membandingkan empat *wireless security protocol* yaitu *Open Security*, WEP, WPA dan WPA2 pada jaringan *wireless* 802.11ac, hasilnya menunjukan bahwa pada TCP dengan IPv4 penggunaan WEP menurunkan *throughput* sebesar 16.17%, WPA sebesar 24.79% dan WPA2 sebesar 0.64%, dan untuk UDP dengan IPv4 penggunaan WEP menurunkan throughput sebesar 58.22%, WPA sebesar 60.84% dan WPA2 sebesar 55.23% [12].

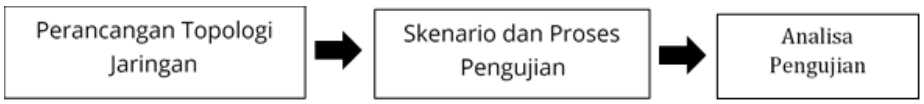
Opportunistic Wireless Encryption (OWE) merupakan salah satu metode yang dapat dimanfaatkan guna meningkatkan keamanan pada jaringan nirkabel yang terbuka. OWE memberikan perlindungan data saat komunikasi berlangsung tanpa memerlukan otentikasi pengguna [13], perlindungan data dilakukan melalui mekanisme pertukaran *public key* antara perangkat yang digunakan oleh pengguna dengan perangkat access point menggunakan algoritma *Elliptic Curve Diffie-Hellman* (ECDH) dan menghasilkan *Pairwise Master Key* (PMK) unik untuk setiap sesi komunikasi [14], sehingga melalui mekanisme perlindungan data tersebut dapat meningkatkan keamanan jaringan publik untuk penggunaan jaringan nirkabel seperti di kafe dan pusat perbelanjaan [15]. Meski menawarkan keunggulan dalam hal keamanan pada jaringan terbuka, implementasi OWE di jaringan 802.11ax masih memerlukan penelitian lebih lanjut untuk memahami dampaknya terhadap kinerja jaringan seperti sejauh mana penggunaan OWE dapat mempengaruhi metrik kinerja jaringan nirkabel seperti *throughput* dan *packet loss*. Sehingga nantinya penggunaan OWE pada jaringan Wi-Fi 6 dapat memberikan wawasan mengenai sejauh mana enkripsi tanpa otentikasi ini mempengaruhi performa dan keandalan jaringan nirkabel di lingkungan yang memiliki interferensi dengan perangkat jaringan nirkabel lainnya.

Dengan demikian, berdasarkan studi yang telah disampaikan sebelumnya untuk penelitian ini akan menggunakan standar jaringan nirkabel yang baru yaitu 802.11ax dan *wireless security* baru yaitu OWE serta menggabungkan beberapa parameter seperti penggunaan *open security*, metrik pengukuran *throughput*, jenis paket data TCP dan UDP serta penggunaan variasi paket data. Tujuan dari penelitian ini untuk menganalisis penggunaan OWE di jaringan 802.11ax terhadap kualitas layanan (QoS) dalam hal metrik *throughput* dan *packet loss*.

Hasil penelitian diharapkan dapat menjadi dasar bagi pengembangan jaringan nirkabel publik yang lebih aman dan efisien, serta memberikan kontribusi bagi literatur ilmiah terkait keamanan dan performa jaringan 802.11ax.

2. METODE PENELITIAN

Untuk pendekatan di penelitian ini menggunakan eksperimental, untuk menghasilkan kesimpulan berdasarkan hasil tes yang sudah dilakukan selanjutnya hasil pengujian akan dianalisis untuk mendapatkan informasi [11]. Berikut merupakan tahapan yang akan dilakukan di dalam penelitian ini seperti dirangkum dalam Gambar 1.



Gambar 1. Prosedur Yang Dilakukan Dalam Penelitian

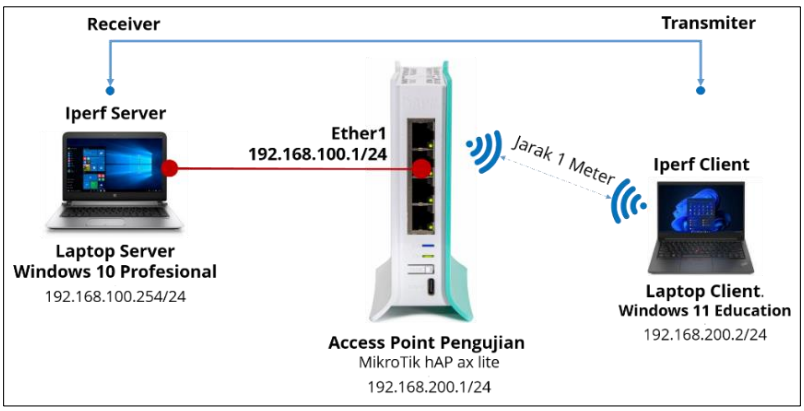
Gambar 1 merupakan prosedur penelitian yang akan dilakukan, terdapat 3 tahapan yang akan dirangkum di bawah ini:

2.1. Perancangan Topologi Jaringan

Untuk skema topologi yaitu *client-server*, dan pada saat pengetesan jaringan akan digunakan dua buah laptop yang masing-masing akan terinstal aplikasi iperf sebagai pengukur *througphut* dan *packet loss*. Untuk laptop pertama akan difungsikan sebagai iperf *client*, menggunakan sistem operasi Windows 11 Education dan terpasang *wireless card* intel® Wi-Fi 6 AX201 yang nantinya terhubung ke jaringan nirkabel melalui MikroTik hAP ax lite sebagai *access point indoor*, sedangkan untuk laptop kedua yang difungsikan sebagai *iperf* server menggunakan sistem operasi Windows 10 Profesional yang terhubung ke MikroTik hAP ax lite melalui kabel jaringan (UTP *category* 6).

Pada penelitian ini, menggunakan gelombang radio 2.4 GHz, yang banyak digunakan [16] seperti contoh di lingkungan pendidikan sekolah [17], sehingga penelitian ini dapat mengukur performa jaringan dan kualitas layanan dalam kondisi nyata dan lingkungan dengan interferensi tinggi.

Selanjutnya jarak antara laptop *client* dengan MikroTik hAP ax lite yaitu 1 meter hal ini bertujuan menjaga sinyal yang di dapat oleh laptop *client* baik [18] seperti dirangkum dalam gambar 2.



Gambar 2. Skema Topologi Untuk Pengujian

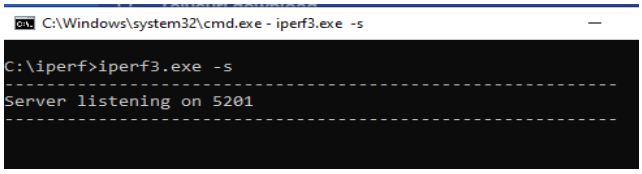
Pengaturan topologi dalam proses pengujian menggunakan protokol alamat IP versi 4 pada tiap perangkat yang terhubung dalam sistem jaringan, dengan laptop server memiliki alamat IP kelas C yaitu 192.168.100.254/24, dan untuk perangkat laptop *client* dengan alamat IP kelas C yaitu 192.168.200.2/24, dan MikroTik hAP ax lite sebagai penghubung dengan alamat IP 192.168.200.1/24. Sejumlah parameter pengujian dirangkum dalam Tabel 1.

Tabel 1. Unsur Penilaian pada Penelitian

Item Parameter	Keterangan
Skema Topologi	*Client Server*
Alamat IP	IPversi4
Jenis Pengamanan Nirkabel	*Open Security, OWE*
Jenis Paket Data	TCP dan UDP
Paket Data TCP	384, 640, dan 1408 KBytes
Paket Data UDP	10, 100, dan 1000 MBytes
Frekuensi	2.4 Ghz
Channel Width	20 Mhz

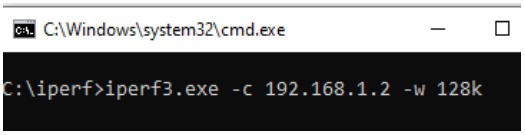
Pada pengujian ini, aplikasi *iperf* versi 3.17 64-bit digunakan untuk memperoleh hasil metrik *throughput* pada jaringan nirkabel. Aplikasi *iperf* 3.17 64-bit ini diinstal pada laptop *client* untuk mendistribusikan trafik dalam paket data tertentu ke laptop server, yang akan menerima trafik tersebut dalam bentuk nilai *throughput*. Pengujian dilakukan dalam kondisi jaringan yang mengalami interferensi[11].

Pada penelitian ini menggunakan aplikasi iperf [11], [18], perintah yang digunakan untuk menjalankan aplikasi iperf menggunakan *command prompt* Microsoft Windows, perintah konfigurasi ditunjukan pada gambar 3 :



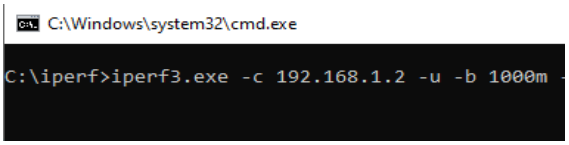
Gambar 3. Perintah *iperf* Pada Laptop Server yang Bertindak sebagai Receiver

Dan berikut merupakan penjelasan perintah di dalam gambar 3 yang digunakan untuk PC Server, perintah iperf.exe merupakan perintah yang digunakan untuk memanggil aplikasi *iperf* yang sebelumnya telah disimpan di drive C:\ dengan folder *iperf*. kemudian untuk perintah –s digunakan agar aplikasi ini berjalan sebagai mode Server (receiver). Nantinya baik pada mode server maupun *clien*t akan menggunakan port 5201 ketika pengujian protokol TCP dan UDP, yang mana port 5201 adalah *port default iperf* versi 3.17 64-bit.



Gambar 4. Perintah *iperf* Pada Laptop *Client* yang Bertindak sebagai Transmitter untuk Pengujian TCP

Selanjutnya untuk penjelasan perintah di dalam gambar 4 yang digunakan pada laptop *client* untuk pengujian protokol TCP, perintah iperf.exe merupakan perintah yang digunakan untuk memanggil aplikasi *iperf* yang sebelumnya telah disimpan di drive C:\ dengan folder *iperf*. kemudian untuk perintah –c digunakan agar aplikasi ini berjalan sebagai mode *client* (transmitter). alamat IP address 192.168.100.254 adalah alamat IP address PC Server yang menjalankan *iperf* dalam mode server, dan untuk perintah –w merupakan perintah yang digunakan untuk mengatur ukuran paket yang akan dikirimkan dan diikuti dengan menuliskan ukuran paket yang akan dikirimkan yaitu 384 KB, 640 KB, 1408 KB.



Gambar 5. Perintah iperf Pada Laptop *client* yang bertindak sebagai transmitter untuk pengujian UDP

Kemudian perintah yang digunakan untuk pengujian UDP seperti ditunjukan di gambar 5, perintah iperf.exe merupakan perintah yang digunakan untuk memanggil aplikasi iperf yang sebelumnya telah disimpan di drive C:\ dengan folder iperf. kemudian untuk perintah –c digunakan agar aplikasi ini berjalan sebagai mode client (transmitter). alamat IP 192.168.100.254 adalah alamat IP address laptop Server yang menjalankan *iperf* dalam mode server, perintah –u digunakan untuk berjalan di mode UDP, perintah –b digunakan untuk memberikan ukuran bandwidth pada UDP sebanyak 1000 Mbits.

Untuk mencapai hasil optimal penggunaan perangkat keras laptop menjadi salah satu aspek yang dipertimbangkan dalam pengujian yang digunakan sebagai server dan *client*, dirangkum dalam Tabel 2.

Tabel 2. Spesifikasi Perangkat Laptop Untuk Pengujian

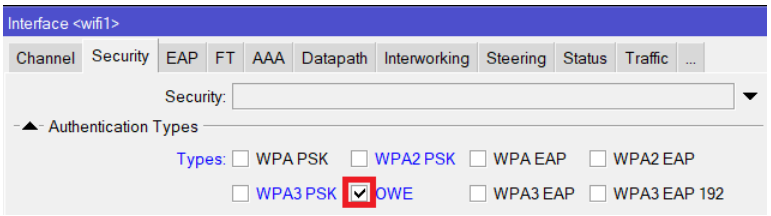
Komponen	Kegunaan	Spesifikasi Detail Perangkat
Laptop Hewlett Packard Probook 440 G3	*Server*	Menggunakan IntelCore i5 seri 6200U kecepatan 2.3 -2.8 GHz, kapasitas media penyimpanan berupa Solid State Drive 128GB, Kapasitas memory sebesar 16384 MB, Realtek Ethernet (10/100/1000)
Laptop Lenovo Thinkpad E14	*Client*	Intel® Core i5-1335U kecepatan 1.30 Ghz, kapasitas Memory 8 GB, kapasitas media penyimpanan berupa Solid State Drive 256 GB, Wireless chipset intel® Wi-Fi 6 AX201.

MikroTik hAP ax lite yang bertindak sebagai penghubung akses jaringan melalui koneksi jaringan nirkabel selanjutnya memiliki spesifikasi yang dijelaskan dalam Tabel 3.

Tabel 3. Detail teknis MikroTik hAP ax lite dalam fungsi sebagai *Access Point.*

Komponen	Kegunaan	Spesifikasi Detail Perangkat
MikroTik hAP ax lite	*Wireless Access Point*	Menggunakan CPU ARM running at 800 MHz, 4x Gigabit Ethernet ports, Wireless Standarts support Wi-Fi 6, Power TX of Wireless 27dBm, Operating System RouterOS v7

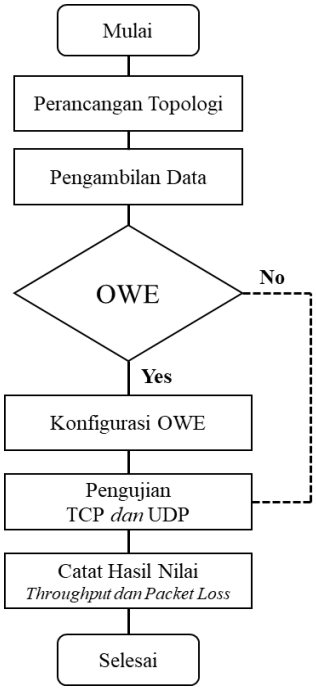
Kemudian untuk penggunaan OWE di MikroTik, melalui parameter *security* di *interface Wifi* dan pada bagian *authentication types* menggunakan OWE seperti dirangkum dalam gambar 6.



Gambar 6. Penggunaan OWE di MikroTik

2.2. Skenario dan Proses Pengujian

Tujuan penggunaan skenario eksperimen yang dijalankan adalah mendapatkan pengetahuan mengenai dampak penggunaan OWE di jaringan nirkabel 802.11ax dengan metrik pengukuran *throughput* dan *packet loss* serta mendapatkan pemahaman mendalam terkait lingkungan pengujian yang aman dan efektif [19]. Gambar 7 menyajikan kerangka penelitian yang menggambarkan kerangka kerja skenario pengujian.



Gambar 7. Rencana Pengujian

Proses pengujian dibagi menjadi dua tahap untuk memperoleh data throughput dan packet loss dalam jaringan nirkabel IEEE 802.11ax dengan skenario penerapan *Opportunistic Wireless Encryption* (OWE) dan *Open Security*. Pada tahap pertama, pengujian dilakukan untuk mengukur *throughput* maksimum. Dalam pengujian ini, dua laptop digunakan, yaitu satu laptop sebagai *iperf client* yang berfungsi mengirimkan data, dan satu lagi sebagai *iperf* server yang menerima data. Laptop *iperf client* dikonfigurasi untuk mengirimkan paket data berbasis protokol TCP *Window* dengan ukuran paket sebesar 384 Kbps, 640 Kbps, dan 1408 Kbps ke laptop *iperf* server. Setiap konfigurasi ukuran paket data dikirimkan sebanyak 10 kali, dengan durasi pengiriman 10 detik untuk setiap kali pengiriman. Hasil *throughput* yang diukur selama pengujian ini akan dibandingkan antara skenario OWE dan *Open Security* untuk menganalisis pengaruh skenario keamanan terhadap kinerja jaringan.

Tahap kedua difokuskan pada pengujian *packet loss* dengan menggunakan protokol UDP. Dalam pengujian ini, laptop *iperf client* dikonfigurasi untuk mengirimkan data dengan ukuran 10 MB, 100 MB, dan 1000 MB ke laptop *iperf* server. Sama seperti pada tahap pertama, pengiriman data dilakukan sebanyak 10 kali, dengan durasi 10 detik untuk setiap kali pengiriman. Data yang diterima oleh laptop *iperf* server kemudian dicatat, dan jumlah *packet loss* dihitung dengan membandingkan jumlah paket yang dikirim dengan jumlah paket yang diterima. Hasil *packet loss* dari setiap skenario OWE dan *Open Security* akan dianalisis untuk memahami perbedaan reliabilitas jaringan antara kedua skenario keamanan tersebut. Seluruh hasil pengujian dari kedua tahap ini nantinya akan disajikan dalam bentuk tabel atau grafik untuk memudahkan interpretasi dan pengambilan kesimpulan.

2.3. Analisis Pengujian

Setelah data-data yang diperlukan terkumpul, selanjutnya, tahap yang dilakukan adalah menganalisis untuk memproses data tersebut sehingga menghasilkan kesimpulan dan informasi [20]. Analisis yang dilakukan adalah berdasarkan data pengujian yang telah dilakukan yaitu membandingkan kualitas jaringan nirkabel 802.11ax ketika menggunakan OWE dan *Open Security* dengan variasi penggunaan parameter TCP *protocol* dan UDP *protocol* serta pengiriman jumlah paket data. Dan berikut merupakan langkah-langkah yang dilakukan:

a. Melakukan Identifikasi Data Hasil Pengujian

Data yang diperoleh dari pengujian adalah sebagai berikut:

1) *Throughput* maksimum: Mengukur kapasitas maksimum jaringan dalam mentransfer data dalam satuan bit per detik (bps). Data ini diperoleh dengan menjalankan protokol TCP dan UDP pada masing-masing skenario (OWE dan *Open Security*).
2) *Packet loss*: Mengukur jumlah paket data yang hilang selama proses pengiriman dibandingkan dengan jumlah paket yang dikirimkan. Parameter ini sangat penting untuk menilai reliabilitas jaringan.

b. Melakukan Pengelompokan Berdasarkan Skenario Pengujian :
   1) Skenario pertama terkait keamanan OWE (*Opportunistic Wireless Encryption*): Analisis difokuskan pada bagaimana OWE mempengaruhi *throughput* maksimum dan *packet loss* dengan protokol TCP dan UDP.
   2) Skenario kedua terkait keamanan *Open Security*: Data dianalisis untuk melihat kinerja jaringan tanpa enkripsi sebagai pembanding.
c. Melakukan Pengujian dengan Protokol TCP dan UDP
   1) Protokol TCP: Mengukur *throughput* dan *packet loss* dalam koneksi yang menggunakan mekanisme kontrol transmisi, seperti pengelolaan ulang jika ada paket yang hilang. TCP cenderung menghasilkan reliabilitas tinggi tetapi diperkirakan mempengaruhi *throughput*.
   2) Protokol UDP: Mengukur performa jaringan dalam pengiriman data yang tidak memiliki kontrol transmisi, yang biasanya menghasilkan *throughput* tinggi tetapi rawan *packet loss*.
d. Melakukan Perbandingan Data
   1) Data *throughput* dan *packet loss* dibandingkan antara protokol TCP dan UDP dalam skenario OWE dan *Open Security*.
   2) Analisis dilakukan untuk mengidentifikasi pola, seperti apakah OWE menurunkan *throughput* dibandingkan *Open Security* atau apakah OWE menghasilkan packet loss yang lebih besar.
e. Melakukan Analisis Berdasarkan Hasil Pengujian
   1) *Throughput* maksimum: Mengidentifikasi faktor-faktor yang memengaruhi *throughput*, seperti overhead dari enkripsi OWE.
   2) *Packet loss*: Menganalisis penyebab hilangnya paket, seperti kualitas sinyal, gangguan jaringan, atau mekanisme enkripsi.
f. Melakukan Visualisasi dan Interpretasi Data
   Data hasil pengujian disajikan dalam bentuk tabel dan grafik untuk mempermudah interpretasi. Dan berikut visualisasi data yang digunakan:
   1) Grafik perbandingan *throughput* maksimum antara OWE dan *Open Security* untuk setiap protokol.
   2) Grafik perbandingan *packet loss* berdasarkan variasi jumlah paket data.

3. HASIL DAN PEMBAHASAN

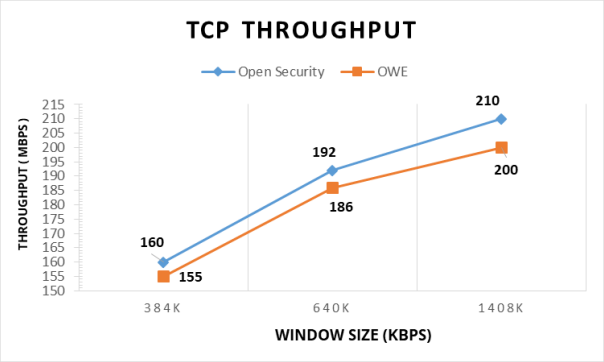
3.1 Pengujian Mode *Open Security* dan OWE Untuk *Metrik Throughput*

Pada pengujian pertama dilakukan dengan tujuan untuk mendapatkan nilai *throughput* yang dihasilkan ketika menggunakan *wireless security Open Security* dan OWE, penggunaan variasi paket TCP *window size* yang dikirimkan terdiri dari ukuran 384 *kilobyte*, 640 *kilobyte*, dan 1408 *kilobyte* dari laptop yang terinstal *iperf mode client* menuju laptop yang terinstal *iperf mode* server dan saling terhubung melalui hAP ax lite. Pengukuran *throughput* dilakukan melalui 10 pengujian pengiriman data, di mana setiap pengujian berlangsung selama 10 detik. Jarak antar laptop yang terinstal iperf *mode client* dengan hAP ax lite yaitu 1 meter. Dan berikut data hasil pengujian perbandingan penggunaan *Open Security* dan OWE untuk metrik *throughput* dirangkum pada Tabel 4.

Tabel 4. Hasil Pengujian Perbandingan Penggunaan *Open Security* dan OWE Untuk Metrik *Throughput*

Pengujian Ke	Open Security			OWE		
	384k	640k	1408	384k	640k	1408
1	166	191	223	160	190	201
2	155	187	192	185	200	199
3	131	202	195	179	200	203
4	169	201	204	115	176	191
5	165	195	214	120	179	203
6	156	184	219	148	188	196
7	150	191	219	130	186	204
8	151	185	203	181	181	202
9	187	196	206	161	183	197
10	166	184	220	171	175	200
Rata-rata	**160**	**192**	**210**	**155**	**186**	**200**

Selanjutnya grafik hasil pengujian perbandingan penggunaan *Open Security* dan OWE untuk metrik *throughput* ditunjukan pada Gambar 8.



Gambar 8. Grafik perbandingan *Open Security* dan OWE untuk Metrik *Throughput*

Berdasarkan Gambar 7, menunjukan bahwa pada saat pengiriman paket dengan ukuran *window size* 384 KB, Open Security memiliki nilai *throughput* sebesar 160 Mbps, sedangkan OWE sedikit lebih rendah yaitu 155 Mbps. Selisih *throughput* antara keduanya adalah 5 Mbps. Pada paket *window size* ini, perbedaan antara *Open Security* dan OWE sangat kecil, menunjukkan bahwa keduanya memberikan performa yang hampir sama. Selanjutnya pada saat pengiriman paket dengan ukuran *window size* 640 KB, *Open Security* memiliki nilai *throughput* sebesar 192 Mbps, sedangkan OWE lebih rendah yaitu 186 Mbps, selisih *throughput* antara keduanya sebesar 6 Mbps. Perbedaan lebih terlihat dalam pengujian paket data ini, di mana *Open Security* memberikan performa yang sedikit lebih tinggi dibanding OWE. Hal ini menunjukkan bahwa *Open Security* lebih optimal pada kecepatan menengah ini. Berikutnya adalah saat pengiriman paket dengan ukuran *window size* 1408 KB, *Open Security* memiliki nilai *throughput* sebesar 210 Mbps, sedangkan OWE lebih rendah yaitu 200 Mbps, selisih *throughput* antara keduanya sebesar 10 Mbps. Seperti halnya pada pengujian dengan ukuran paket 384KB dan 640 KB, pada pengujian paket data 1408KB menunjukkan bahwa pengiriman paket data semakin besar penurunan performa yang lebih signifikan pada OWE dibandingkan *Open Security*.

3.2 Pengujian Mode Open Security dan OWE Untuk Metrik Packet Loss

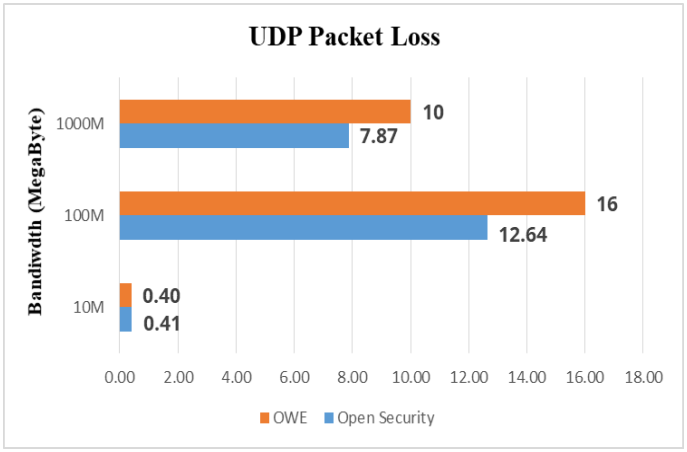
Seperti halnya pada pengujian pertama, untuk pengujian kedua ini dilakukan dengan tujuan untuk memperoleh nilai *packet loss* yang dihasilkan ketika menggunakan jenis keamanan jaringan nirkabel *Open Security* dan OWE, penggunaan variasi paket UDP yang dikirimkan terdiri dari ukuran 10 MB, 100 MB, dan 1000 MB dari laptop yang terinstal *iperf client* menuju laptop yang terinstal *iperf* server dan saling terhubung melalui hAP ax lite. Pengukuran *throughput* dilakukan dengan mengirim data sebanyak 10 kali, dengan durasi 10 detik untuk setiap pengujian.

Penggunaan jarak juga telah ditentukan yaitu antara laptop yang terinstal *iperf client* dengan hAP ax lite adalah 1 meter. Dan berikut data hasil pengujian perbandingan penggunaan *Open Security* dan OWE untuk metrik *packet loss* dirangkum dalam Tabel 5.

Tabel 5. Hasil Pengujian Perbandingan Penggunaan *Open Security* dan OWE Untuk Metrik *Packet Loss*

Pengujian Ke	Open Security			OWE		
	10 M	100 M	1000 M	10 M	100 M	1000 M
1	1.1	26	7.9	0.29	19	6
2	0.57	28	7.8	0.58	6	4.7
3	0.035	11	8.4	1.1	4.8	7.2
4	0	22	9.5	0	29	12
5	0.57	1	7	1.2	12	14
6	0.082	5.5	7.5	0.35	23	11
7	0	9.5	7.2	0	12	14
8	0.49	7	8.6	0.57	15	16
9	0.2	7.1	6.4	0	13	6.8
10	0.97	9.3	8.4	0	23	6.5
Rata-rata	**0.40**	**12.64**	**7.87**	**0.41**	**16**	**10**

Selanjutnya grafik hasil pengujian perbandingan penggunaan *Open Security* dan OWE untuk metrik *packet loss* ditunjukan pada Gambar 9.



Gambar 9. Grafik perbandingan *Open Security* dan OWE untuk Metrik *Packet Loss*

Berdasarkan Gambar 9 menunjukan bahwa pada ukuran *bandwitdh* 10 MB, perbedaan antara OWE dan *Open Security* tidak terlalu signifikan. Hal ini menunjukkan bahwa pada ukuran *bandwith* kecil, keduanya cukup andal dalam menangani lalu lintas UDP tanpa mengalami banyak kehilangan paket, pada OWE kehilangan data sebesar 0.40% dan *Open Security* 0.41%. Selanjutnya pada *bandwitdh* dengan ukuran 100 MB, kehilangan paket meningkat secara signifikan baik pada OWE maupun *Open Security*. Namun, pada *Open Security* memiliki tingkat perfoma yang lebih baik dibandingkan OWE, dengan kehilangan paket yang lebih rendah sekitar 3.36 %. Pada pengujian *bandwidth* dengan ukuran 1000 MB, kehilangan paket tidak meningkat secara signifikan seperti pada pengujian *bandwidth* dengan ukuran 100 MB data, hal ini menunjukkan bahwa jaringan 802.11ax dapat menangani jumlah data yang jauh lebih besar. Namun masih terdapat perbedaan antara OWE dan *Open Security*, hasil pengujian pada *Open Security* memiliki performa yang lebih baik dibandingkan OWE. Kehilangan paket saat menggunakan *Open Security* sebesar 7.87 % sedangkan pada OWE sebesar 10%, hal ini menunjukkan bahwa mekanisme *open security* lebih efisien dalam menangani lalu lintas UDP yang berisi data dalam jumlah besar. Penggunaan OWE memberikan keamanan dalam lalu lintas data karena adanya enkripsi, namun juga menimbulkan *overhead* tambahan [21] sehingga meningkatkan kehilangan paket yang dikirimkan.

4. KESIMPULAN DAN SARAN

Setelah melalui proses pengujian, berikut adalah poin-poin kesimpulan yang dapat diambil bahwa, hasil dari pengujian untuk nilai metrik *throughput* menunjukan *Open Security* secara konsisten menghasilkan *throughput* yang sedikit lebih tinggi dibandingkan OWE. Pada pengujian dengan ukuran paket TCP window 384 KB, 640 KB, dan 1408 KB, *Open Security* memberikan hasil nilai *throughput* berturut-turut sebesar 160 Mbps, 192 Mbps, dan 210 Mbps, sementara saat menggunakan OWE mengalami penurunan dengan selisih 5 hingga 10 Mbps. Hasil ini mengindikasikan bahwa ketika jaringan nirkabel menggunakan OWE mengalami sedikit penurunan performa seiring dengan peningkatan ukuran paket. Penurunan ini menunjukkan bahwa *overhead* enkripsi pada OWE dapat mempengaruhi kinerja, terutama pada ukuran paket yang besar.

Hasil dari pengujian terhadap metrik *packet loss* menunjukan bahwa dalam hal kehilangan paket, *Open Security* juga menunjukkan performa yang lebih baik dibandingkan OWE, terutama pada ukuran data yang lebih besar. Pada ukuran paket UDP 10 MB, perbedaan *packet loss* antara OWE (0.40%) dan *Open Security* (0.41%) sangat kecil, menunjukkan bahwa keduanya cukup andal pada data yang kecil. Namun, ketika ukuran paket ditingkatkan menjadi 100 MB, *packet loss* pada *Open Security* tercatat lebih rendah sekitar 3.36% dibandingkan OWE. Pada ukuran data 1000 MB, *packet loss* pada *Open Security* mencapai 7.87%, sedangkan pada OWE sebesar 10%. Hal ini menunjukkan bahwa *Open Security* lebih efisien dalam menangani lalu lintas UDP dengan ukuran data yang besar, sementara *overhead* enkripsi pada OWE cenderung menambah jumlah kehilangan paket.

DAFTAR PUSTAKA

[1] D. N. Astrida, A. R. Saputra, and A. I. Assaufi, "Analysis and Evaluation of Wireless Network Security with the Penetration Testing Execution Standard (PTES)," *SinkrOn*, vol. 7, no. 1, pp. 147-154, 2022.

[2] M. Natkaniec and N. Bieryt, "An Analysis of the Mixed IEEE 802.11ax Wireless Networks in the 5 GHz Band," *Sensors*, vol. 23, no. 10, pp-1-34, 2023.

[3] G. Z. Islam and M. A. Kashem, "Efficient resource allocation in the IEEE 802.11ax network leveraging OFDMA technology," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 2, pp. 1-9, 2022.

[4] S. Maesaroh, L. Kusumaningrum, N. Sintawana, D. P. Lazirkha, and R. D. O., "Wireless Network Security Design And Analysis Using Wireless Intrusion Detection System," *Intnational Journal Cyber IT Service Management*, vol. 2, no. 1, pp. 30–39, 2022.

[5] M. A. Adiguna and B. W. Widagdo, "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r)," *Jurnal Sistem Komputer dan Kecerdasan Buatan (SISKOM-KB)*, vol. 5, no. 2, pp. 1-8, 2022.

[6] M. Y. Efendi and I. Riadi, "Analisis Perbandingan Metode Keamanan Wireless WEP 128bit Dan WPA Untuk Meningkatkan Keamanan Wireless," *Jurnal Sarjana Teknik Informatika*, vol. 7, no. 1, pp. 63-68, 2019.

[7] D. Steiner-Otoo and H. Jahankhani, "*An Investigation into How Smartphones Can Be Secured Against MiTM Attacks: Financial Sector*," in book series: Advanced Sciences and Technologies for Security Applications (ASTSA), pp. 171-215, 2022.

[8] I. Riadi, H. Herman, and A. Z. Ifani, "Prototype Pengembangan Aplikasi Login menggunakan Teknologi Blockchain," *Journal of Applied Informatics and Computer*, vol. 5, no. 1, pp.1-8, 2021.

[9] S. Z. Mosawi, M. Qasimi, W. M. Wadeed, and K. R. Rahmani, "Exploring Wi-Fi Security Challenges and Proposing Solutions: The case of Afghanistan," EJECE: *European Journal of Electrical Engineering & Computer Science*, vol 7, 5, pp. 1-19, 2023.

[10] A. Halbouni, L. Y. Ong, and L. M. Chew, "Wireless Security Protocols WPA3: A Systematic Literature Review," *IEEE Access*, vol. xx, pp. 1-1, 2023.

[11] V. A. Saputro, S. Raharjo, and E. Pramono, "Pengaruh Wireless Security Protocol Pada Throughput Jaringan Wireless 802.11ax," vol. 23, no. 2, pp. 1–7, 2021.
[12] T. M. Alghamdi, "Throughput Analysis of IEEE WLAN '802.11 ac' Under WEP, WPA, and WPA2 Security Protocols," *International Journal of Computer Networks (IJCN)*, vol. 9, no. 1, pp. 1-13, 2019.
[13] R. Badhwar, "Next Gen Wi-Fi and Security," in *The CISO's Next Frontier*, 2021.
[14] S. Kwon and H. K. Choi, "Evolution of Wi-Fi Protected Access: Security Challenges," *IEEE Consumer Electronics Magazine*, vol. 10, no. 1, pp. 74-81, 2021.
[15] G. D. Migration, "Planning Guide Appendix A : Documentation References."
[16] Yusantono, "Analisis dan Perbandingan Jaringan WiFi dengan frekuensi 2.4 GHz dan 5 GHz dengan Metode QoS," *Journal of Information System Technology*, vol. 05, no. 05, pp. 34–52, 2020.
[17] A. S. Amin, K. Harsanto, and R. Samsinar, "Implementasi Jaringan Kabel Dan Wireless Menggunakan Router Mikrotik Pada Sd Muhammadiyah 1 Jakarta," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 5, no. 2, pp. 255–264, 2022.
[18] V. A. Saputro and S. Raharjo, "Pengaruh Penggunaan Beacon Interval Dalam Meningkatkan Throughput Jaringan Wireless IEEE 802.11ax," *Jurnal Sistem Komputer dan Kecerdasan Buatan (SISKOM-KB)*, vol. 6, no. 1, pp. 29-36, 2022.
[19] Z. Alamsyah, G. P. Insany, and F. J. Taqwana, "Perancangan Dan Implementasi Aplikasi Keamanan Ujian Online Menggunakan Algoritma Rijndael Dan Remote Desktop Protocol," *SKANIKA Sistem Komputer dan Teknik Informatika*, vol. 7, no. 2, pp. 119–132, 2024.
[20] I. Priambudi and M. Mufti, "Implementasi Kriptografi Dengan Metode Aes-128 Untuk Pengamanan File Berbasis Web Pada Smp Yapipa," *SKANIKA: Sistem Komputer dan Teknik Informatika*, vol. 6, no. 1, pp. 22–31, 2023.
[21] K. Murugesan, K. K. Thangadorai, and V. N. Muralidhara, "PoEx: Proof of Existence for Evil Twin Attack Prevention in Wi-Fi Personal Networks," *2021 8th International Conference on Future Internet of Things and Cloud (FiCloud)*, Aug 2021.