Jurnal Sistem Komputer dan Kecerdasan Buatan
Vol.VI No.1 September Tahun 2022

Pengaruh Penggunaan Beacon Interval Dalam Meningkatkan Throughput Jaringan Wireless IEEE 802.11ax

Vian Ardiyansyah Saputro[1], Suwanto Raharjo[2]
[1]Politeknik AstraManajemen Informatika
[2]IST AKPRIND Yogyakarta/Informatika
vian.ardiyansyah@polman.astra.ac.id[1], wa2n@akprind.ac.id[2]

Diterima : 22 Agustus 2022
Disetujui : 01 Oktober 2022

***Abstract*— Standarisasi IEEE 802.11ax yang lebih dikenal WiFi 6 merupakan regulasi teknologi jaringan wireless terbaru yang dikeluarkan oleh IEEE sebagai pengembangan dari standar jaringan wireless IEEE 802.11ac. Tidak seperti halnya pada jaringan kabel, jaringan wireless memiliki kerentanan terhadap keamanan pengguna jaringan dikarenakan sifat jaringan wireless yang lebih terbuka sehingga memungkinkan siapa saja dapat mengakses jaringan wireless tersebut, Salah satu cara yang dapat dilakukan untuk mengamankan jaringan wireless adalah dengan menerapkan wireless security protocols dimana tersedia berbagai mode yang dapat digunakan, salah satunya adalah mode WPA3-SAE namun di dalam penggunaan wireless security protocols ini dapat menurunkan throughput yang didapatkan oleh pengguna jaringan wireless dengan adanya penurunan throughput ini tentunya akan mengakibatkan performa jaringan wireless menjadi tidak maksimal. Tujuan utama di dalam penelitian ini adalah untuk mengetahui bagaimana penggunaan beacon interval dalam meningkatkan throughput ketika menerapkan wireless security protocol di jaringan wireless dengan standar IEEE 802.11ax. Hasil yang kami dapatkan menunjukan bahwa perubahan nilai beacon interval saat menerapkan wireless security protocols mode Open Security dapat meningkatkan throughput hingga 0,7 % dan 0,6 % saat menerapkan mode WPA3-SAE.**

***Keywords* — wireless, 802.11ax, beacon interval, throughput, wpa versi 3-sae**

I. PENDAHULUAN

A. Latar Belakang Permasalahan

Penggunaan jaringan nirkabel saat ini sangat menjanjikan dan populer baik di lingkungan sekolah, perkantoran, bahkan di lingkungan industri, salah satu pemanfaatan dari jaringan nirkabel adalah untuk media komunikasi dan berbagi data antar perangkat yang saling terkoneksi sehingga diharapkan dapat meningkatkan produktifitas kerja [1]. Seperti kita ketahui bersama IEEE di tahun 2019 mengeluarkan standar nirkabel terbaru yaitu IEEE 802.11ax, dimana di dalam standar baru ini menawarkan berbagai fitur baru di antaranya adalah kecepatan nirkabel yang ditawarkan mencapai 9,6 Gbps saat digunakan di *channel width* 160 Mhz, dan juga dapat bekerja di frekuensi 2.4 Ghz dan frekuensi 5 Ghz, selain itu juga adalah pembaruan dari sisi keamanan yaitu adanya protokol keamanan baru yang kita kenal dengan WPA versi 3 - SAE. Berbeda halnya dengan jaringan kabel, jaringan nirkabel memiliki kerentanan terhadap keamanan pengguna jaringan dikarenakan sifat jaringan nirkabel yang lebih terbuka [2] sehingga memungkinkan siapa saja dapat mengakses jaringan nirkabel tersebut [3]. Penggunaan protokol keamanan di dalam jaringan nirkabel merupakan cara yang umum dilakukan untuk mengamankan jaringan nirkabel dimana tersedia berbagai mode yang dapat digunakan, salah satunya adalah mode WPA versi 3 - SAE namun di dalam penggunaan nirkabel *security protocols* ini dapat menurunkan *throughput* yang didapatkan oleh pengguna jaringan nirkabel [4] dengan adanya penurunan *throughput* ini

tentunya akan mengakibatkan performa jaringan nirkabel menjadi tidak maksimal [5].

Tujuan utama di dalam penelitian ini adalah untuk mengetahui bagaimana penggunaan *beacon interval* dalam meningkatkan *throughput* ketika mengimplementasikan protokol keamanan di jaringan nirkabel standarisasi IEEE 802.11ax, seperti halnya penelitian yang dilakukan [6]. Pada penelitian tersebut bertujuan untuk mengetahui dampak dari penggunaan *beacon interval* di jaringan *nirkabel* standar IEEE 802.11 untuk penggunaan aplikasi di jaringan oportunistik.

Penelitian yang akan dilakukan diharapkan memberikan manfaat bagi ilmu pengetahuan terbaru terkait bagaimana penggunaan *beacon interval dapat* memberikan dampak terhadap kualitas *throughput* jaringan nirkabel standarisasi IEEE 802.11ax.

B. Rumusan Masalah

Dengan adanya permasalahan di dalam penelitian yang telah disampaikan di latar belakang maka dapat dirumuskan permasalahan sebagai berikut:

a. Bagaimanakah efektifitas penggunaan *beacon interval* dalam meningkatkan *throughput* ketika menerapkan nirkabel *security protocol* untuk penggunaan di *channel width* 80 Mhz ?

C. Tujuan

Dengan adanya rumusan masalah yang telah disampaikan, tujuan utama yang ingin dicapai dari penelitian ini adalah Untuk mengetahui efektifitas penggunaan *beacon interval* dalam meningkatkan *throughput* ketika menerapkan nirkabel *security protocol* untuk penggunaan di *channel width* 80 Mhz ?

D. Manfaat

Berikut manfaat yang dapat diperoleh dari laporan hasil penelitian ini adalah :

a. Dapat membantu para peneliti dan pengguna dalam pemilihan nirkabel *security protocols* khususnya WPA3 dengan enkripsi SAE di dalam merancang dan membangun jaringan nirkabel menggunakan standarisasi IEEE 802.11ax.
b. Mendapatkan pengetahuan mengenai kualitas *throughput* dan keunggulan dari jaringan nirkabel 802.11ax.
c. Mendapatkan pengetahuan mengenai pengaruh penggunaan *beacon interval* di dalam jaringan nirkabel.

II. LANDASAN TEORI

A. Penelitian Terkait

Berdasarkan penelitian sebelumnya terkait analisis kualitas *throughput* jaringan nirkabel 802.11ac berdasarkan penggunaan WEP, WPA dan WPA2 yang dilakukan oleh [7], menunjukkan bahwa kualitas *throughput* data yang dihasilkan ketika jaringan nirkabel tidak menerapkan sistem keamanan hasilnya lebih tinggi dibandingkan ketika sistem keamanan diterapkan di dalam jaringan nirkabel. Untuk protokol TCP penurunan sebesar 16.17% ketika menerapkan WEP, 24,79% (WPA) dan 0.64% (WPA2) sedangkan untuk protokol UDP penurunan sebesar 58,22% (WEP), 60,84% (WPA) dan 55,23% (WPA2). Metode pengujian menggunakan skenario jaringan *client server*, dimana PC *client* akan mengirimkan paket data dengan variasi 128, 384, 640, 896, 1152, & 1408 (Bytes) ke PC *Server* untuk melihat hasil kualitas *throughput* yang didapatkan.

Hal yang sama juga dilakukan oleh [8] melakukan penelitian mengenai dampak penggunaan WEP, WPA, dan WPA2 terhadap kualitas *throughput* jaringan nirkabel 802.11ac dengan membandingkan parameter penggunaan IPv4 dan IPv6, penelitian ini menunjukan ketika *wireless security protocol* WEP, WPA, dan WPA versi 2 digunakan terhadap IPv4 begitu juga IPv6 menunjukan bahwa penggunaan IPv4 lebih stabil dibandingkan IPv6, dimana kualitas *throughput* yang dihasilkan ketika menerapkan WEP sebesar 21.70 Mbps (IPv4) dan 19.40 Mbps (IPv6), kemudian untuk penerapan WPA sebesar 119.00 Mbps (IPv4) dan 113,80 Mbps (IPv6) selanjutnya untuk penerapan WPA2

sebesar 118.00 Mbps (IPv4) dan 115.20 Mbps (IPv6).

Selanjutnya penelitian dilakukan oleh [9] penelitian ini bertujuan untuk mengetahui dampak penggunaan protokol keamanan WPA2 (WiFi Protected Access 2) dan open system (No security) terhadap kualitas *throughput* jaringan nirkabel IEEE 802.11 ac, dimana variable penelitian membandingkan kualitas *throughput* yang didapatkan ketika menggunakan protokol TCP / UDP dengan penggunaaan IPv4 / IPv6. penelitian ini menunjukkan bahwa, ketika jaringan nirkabel mengimplementasikan sistem keamanan WPA2, kualitas *throughput* pada protokol TCP dan penggunaan IPv4 dan IPv6 rata-rata mengalami penurunan sebesar 16,79% dan 10,22%. sedangkan *throughput* untuk UDP menurun sebesar 18.07% dan 12,99% untuk penggunaan IPv4 dan IPv6.

Sehingga dari penelitian yang sebelumnya telah disampaikan maka penulis akan melakukan penelitian berdasarkan konsep yang dilakukan oleh [8]. Selanjutnya pada penelitian yang dilakukan oleh [6] terkait perubahan nilai *beacon interval* dari nilai *default* 100ms menjadi 200ms di dalam penggunaan jaringan oportunitik, hasilnya menunjukan bahwa perubahan ini dapat meningkatkan kualitas *bandwitdh* yang di peroleh pengguna di dalam jaringan nirkabel.

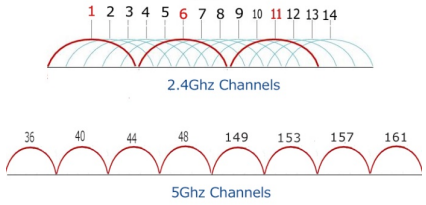
Perbedaan penelitian yang kami lakukan adalah dengan menggunakan standarisasi terbaru yaitu IEEE 802.11ax, kemudian *wireless security protocols* yang digunakan adalah *open security* dan WPA3-SAE, serta nilai *beacon interval* 100ms dan 500ms. Skenario topologi jaringan mengadopsi di dalam penelitian [7] yang menggunakan skenario *client server*.

B. Standarisasi IEEE 802.11ax

WiFi 6 atau standarisasi 802.11ax adalah teknologi jaringan nirkabel terbaru yang memberikan peningkatan signifikan pada standar jaringan nirkabel. Teknologi ini diciptakan sebagai solusi untuk kebutuhan untuk meningkat kan performa dan konektivitas data serta memenuhi kebutuhan *bandwidth* yang besar karena saat ini lebih banyak perangkat yang perlu dihubungkan ke internet. Teknologi WiFi 6 menawarkan fitur baru seperti tersedianya pilihan penggunaan frekuensi 2.4 Ghz dan frekeunsi 5 Ghz, mendukung hingga delapan transmisi MU-MIMO sekaligus [10] dan menggunakan modulasi OFDMA (*Orthogonal Frequency Division Multiple Access*), dimana teknologi ini dapat memulihkan masalah *multi-path* (lintasan jamak) sehingga OFDMA ideal untuk mengatasi lingkungan banyak *obstacle* (penghalang sebagai pemantul) dan lingkungan jaringan nirkabel [11].

C. Channel Width

Lebar pita frekuensi (*channel width*) merupakan lebar saluran untuk menentukan jumlah *bandwidth* yang digunakan di dalam spektrum radio selama proses pengiriman data berlangsung. Keuntungan menggunakan *channel width* yang lebih lebar adalah memungkinkan untuk menghasilkan kecepatan yang lebih tinggi namun terdapat kerugian juga yaitu terjadinya interferensi dengan pemancar lain yang menggunakan *channel width* sama. Pada frekuensi 2.4 Ghz setiap *channel width* memiliki lebar 20 Mhz sedangkan untuk frekuensi 5 Ghz *channel width* sendiri dapat memiliki lebar 20 Mhz, 40 Mhz, 80 Mhz atau 160 Mhz.



Gambar 1. WIFI *Channel bandwidth*

D. Beacon Interval

Beacon interval adalah jarak waktu pengiriman dari *beacon frames*. Perangkat AP mengirimkan dengan jarak waktu yang regular untuk menentukan posisi *user*. Pengaturan otomatis pada perangkat yang digunakan adalah 100 milliseconds (ms) atau 1 detik. Pengaturan ini dapat berbeda tergantung perangkat *Access Point* yang digunakan [12].

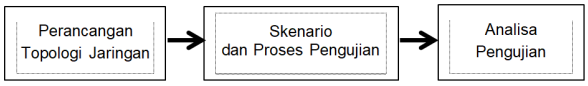
E. WPA versi 3-SAE

WPA versi 3 atau WPA versi 3 merupakan versi pembaruan dari teknologi keamanan nirkabel WPA versi 2. WPA versi 3 dikenalkan ke publik pada 25 Juni 2018, dimana pada WPA versi 3 menggunakan metode enkripsi *Simultaneous Authentication of Equals* (SAE) yang menggantikan metode otentikasi *Pre shared key* [13] dengan enkripsi ini pengguna jaringan nirkabel akan terlindungi dari upaya *brute force* yang dilakukan oleh *attacker*, selain pembaruan

metode enkripsi WPA versi 3 juga menggunakan teknologi *Protected Management Frames* (PMF) yang berguna untuk meningkatkan keamanan dan perlindungan jaringan dari tindakan *spoofing* dan penggunaan enkripsi 192 bit sebagai opsi yang dapat dipilih ketika menggunakan mode WPA3-*Enterprise* [14].

III. METODE PENELITIAN

Di dalam penelitian ini metode yang digunakan berupa eksperimental, yakni dilakukan dengan membuat sebuah eksperimen untuk mendapatkan hasil dari pengujian yang telah dilakukan dan kemudian dilakukan analisis [15]. Selanjutnya tahapan penelitian terbagi menjadi 3 tahapan dan berikut tersebut terlihat pada gambar 2



Gambar 2. Tahapan Penelitian

Gambar 2 merupakan tahapan yang dilakukan dan berikut penjelasan terkait setiap tahapan tersebut.

1. Skenario Topologi Jaringan

Topologi *client server* merupakan skenario topologi yang akan digunakan dimana sistem operasi windows server 2016 standar digunakan untuk PC Server dan sistem operasi windows 10 Pro *build* 2004 digunakan untuk PC *Client* dan pada PC *Client* sudah terpasang *wireless card* TPLink AX3000. Selanjutnya PC *Client* akan terhubung ke *Access Point* TPLink AX73 dengan jarak 1 meter agar dapat mempertahankan kekuatan sinyal sehingga hasil yang didapatkan lebih maksimal [9], dan juga pada penelitian ini digunakan frekuensi 5 Ghz agar mendapatkan hasil *throughput* yang yang lebih tinggi bila dibandingkan saat menggunakan frekuensi 2.4 Ghz [16]

Gambar 3. Perancangan Topologi Jaringan

Pada perancangan topologi jaringan seperti ditunjukan di gambar 3, setiap perangkat yang terhubung seperti PC server, *Access Point* TPLink AX73, dan PC *client* menggunakan pengalamatan IP versi 4 kemudian penggunaan beberapa parameter pengujian diterapkan di dalam skenario pengujian. Berikut beberapa parameter uji yang digunakan dirangkum di dalam tabel 1.

Tabel 1. Parameter Pengujian

Level	Parameter
Tipe Jaringan	*Client Server*
Versi IP Address	IPv4
Protokol Keamanan	*Open Security*, WPA3-SAE
Tipe Paket Data	Paket TCP
Ukuran Paket	128, 640, 1408 (KBytes)
Beacon Interval	100, 500 (Milisecond)

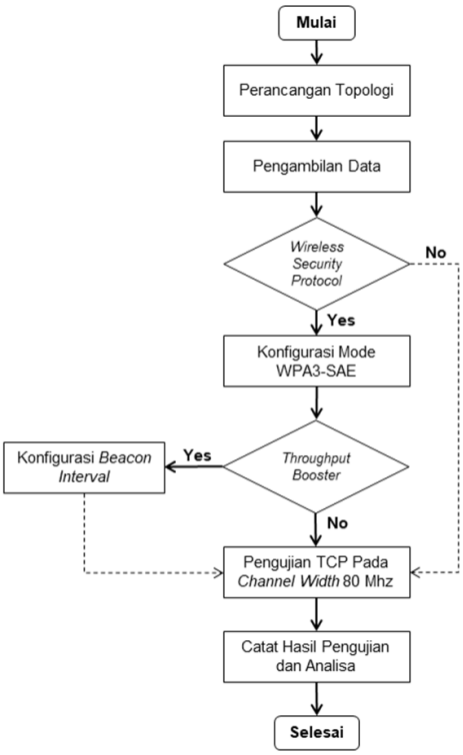
Selanjutnya aplikasi *iperf* untuk mengukur di dalam pengujian ini dimana akan dipasang di PC *client* yang akan mengirimkan paket data dan di PC server yang akan menerima paket data tersebut sehingga akan memberikan hasil berupa nilai *throughput* jaringan nirkabel 802.11ax seperti halnya yang dilakukan oleh [17].
Penggunaan *wireless access point* dan *wireless card adapter* di dalam penelitian ini adalah dengan spesifikasi sebagai berikut :

Tabel 2. Spesifikasi Perangkat

Perangkat Keras	Fungsi	Spesifikasi
TP-Link AX73 (AX5400)	*Wireless Access Point*	Mendukung standar 802.11ax, Dua frekuensi (2.4 GHz and 5 GHz), Gigabit LAN Ports, WPA versi 3 SAE.
TP-Link AX3000 WiFi Card	*Wireless Card Adapter*	Mendukung WiFi 6 dengan kecepatan hingga 2400Mbps, dan Dual frekuensi Wireless.

2. Skenario dan Proses Pengujian

Dengan adanya skenario dan proses pengujian di dalam penelitian ini memiliki tujuan agar didapatkan nilai *throughput* tertinggi saat penerapan *beacon interval* bersamaan dengan penggunaan mode keamanan jaringan *Open Security* dan WPA versi 3 - SAE pada lebar pita 80 Mhz. Dan berikut merupakan tahapan skenario pengujian di dalam gambar 4



Gambar 4. Skenario dan Proses Pengujian

Dan berikut merupakan penjelasan dari setiap tahapan yang dilakukan oleh peneliti :

1. Perancangan Skenario Topologi :
   Di dalam tahapan ini yaitu dengan melakukan desain sebuah topologi yang akan digunakan untuk penelitian. Dengan tujuan agar mendapatkan hasil pengujian sesuai dengan tujuan penelitian.
2. Tahapan pertama dalam pengambilan data (*Wireless Security Protocols*) :
   Seperti halnya pada pengujian yang telah dilakukan oleh [18], di dalam tahap pengujian ini menggunakan protokol TCP dan *channel width* 80 Mhz serta paramater yang akan diuji yaitu *wireless security protocol* mode *Open Security*, dan WPA versi 3 - SAE serta ukuran paket yang akan digunakan adalah 128 KByte, 640 KByte dan 1408 KByte.
3. Tahapan kedua dalam pengambilan data (*Throughput Booster*):
   Seperti halnya pada tahap pertama pada pengambilan data di dalam tahap kedua ini penggunaan parameter uji *wireless security protocols* WPA3-SAE, ukuran paket yang akan digunakan adalah 128 KByte, 640 KByte dan 1408 KByte. serta merubah nilai *beacon interval* menjadi 500 ms seperti halnya pada penelitian yang dilakukan oleh [6] yang menggunakan nilai *beacon interval* 200 ms.

Pengujian setiap paket data yang dikirimkan sebanyak satu kali dengan pengambilan data dilakukan selama 100 detik dan selanjutnya hasil akhir berupa rata-rata di catat ke dalam tabel yang telah dipersiapkan.

3. Analisa Pengujian

Dari pengujian yang telah dilakukan maka akan didapatkan data-data yang diperlukan, untuk langkah selanjutnya adalah melakukan analisis untuk mengolah data tersebut menjadi sebuah informasi. Analisis hasil akan menyajikan perbandingan pada penggunaan protokol TCP. Dimana nantinya analisa yang dilakukan adalah berdasarkan data pengujian dampak penggunaan *beacon interval* untuk meningkatkan *throughput* ketika menggunakan *wireless security protocol* mode *Open Security* dan WPA versi 3 - SAE saat digunakan di *channel width* 80 Mhz.

Selanjutnya untuk teknik analisis data menggunakan *Independent T Test* yaitu menggunakan *z test* untuk melihat perbedaan saat menggunakan nilai *beacon interval* 100 ms dengan 500 ms ketika mengimplementasikan *wireless security protocol*, dimana tingkat signifikansi yang digunakan adalah $\alpha = 5\%$ atau *alpha = 0,05*. Hipotesis penelitian ini berdasarkan parameter yang diselidiki adalah :

H_0 = Tidak ada perbedaan signifikan *throughput* yang dihasilkan ketika menggunakan nilai *beacon interval* 100 ms dengan 500 ms ketika mengimplementasikan *wireless security protocol.*

H_1 = Ada perbedaan signifikan *throughput* yang dihasilkan ketika menggunakan nilai *beacon interval* 100 ms dengan 500 ms ketika mengimplementasikan *wireless security protocol*.

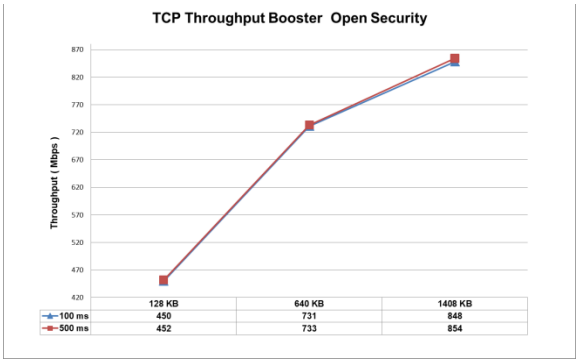
IV. HASIL DAN PEMBAHASAN

1. Hasil Pengujian

Di dalam pengujian ini terdapat 2 skema *wireless security protocol* yang akan digunakan yaitu dengan mode *open security* dan WPA versi 3 - SAE. Dan berikut hasil dan pembahasan dari pengujian yang telah dilakukan :

a. Penggunaan *Beacon Interval* Pada *Open Security*

Throughput booster merupakan metode yang digunakan untuk meningkatkan kualitas *thorughput* yang didapatkan oleh pengguna di jaringan *wireless*, salah satunya adalah dengan melakukan konfigurasi nilai *beacon interval* di dalam *access point*. Pada pengujian untuk protokol TCP dengan penggunaan mode *Open Security* seperti ditunjukan grafik menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat. Dimana nilai *default beacon interval* adalah 100 ms, ketika pengujian diberikan nilai *beacon interval* sebesar 500 ms, *throughput* yang didapatkan mengalami peningkatan hingga 2 Mbps ketika pengiriman paket sebesar 128 KB dan 640 KB serta peningkatan hingga 6 Mbps ketika pengiriman paket sebesar 1408 KB.



Gambar 5. Grafik Penggunaan *Throughput Booster* Pada *Open Security*

b. Penggunaan *Beacon Interval* Pada WPA3-SAE

Selanjutnya pada pengujian untuk protokol TCP dengan penggunaan mode WPA3 - SAE seperti ditunjukan grafik, sama seperti halnya dengan pengujian untuk mode *open security*, pada mode WPA3 – SAE menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat. Perbandingan *throughput* yang didapatkan antara nilai *default beacon interval* 100 ms, dengan ketika pengujian diberikan nilai *beacon interval* sebesar 500 ms, *throughput* yang didapatkan mengalami peningkatan sebesar 2 Mbps ketika pengiriman paket 128 KB dan 1408 KB, serta peningkatan sebesar 4 Mbps ketika pengiriman paket 640 KB.

c. Hasil uji *z test* pengujian hipotesis

Parameter statistik *throughput* untuk implementasi *beacon interval* pada *open security* ditunjukkan pada tabel 3 berikut.

Tabel 3. Statistik *Throughput* untuk *Open Security*

Beacon Interval		Hasil Uji		
100 ms	500 ms	P Value	=	0.969
450	452	Significant	=	Tidak Signifikan
609	613	Mean 100 ms	=	692
731	733	Mean 500 ms	=	696.2
822	829	Perbedaan	=	-4.2
848	854	Kecenderungan	=	Peningkatan

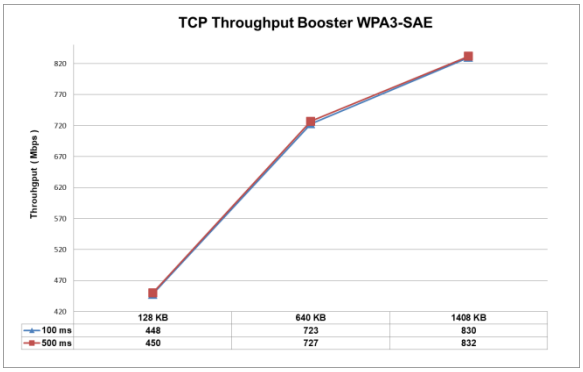
Dari tabel 3 menunjukan bahwa *P value* bernilai 0.969 (p>0.05) hal ini berarti H0 diterima dan H1 ditolak atau dapat diartikan bahwa tidak terdapat perbedaan secara signifikan ketika menggunakan nilai *beacon interval* 100 ms dengan 500 ms ketika mengimplementasikan *wireless security protocol* mode *open security*, akan tetapi memiliki kecenderungan terjadinya peningkatan yaitu perbedaan antara penggunaan 100 ms dengan 500 ms sebesar 4.2.

Selanjutnya pada parameter statistik *throughput* untuk implementasi *beacon interval* pada WPA versi 3 – SAE ditunjukkan pada tabel 4 berikut.

Tabel 4. Statistik *Throughput* untuk WPA versi 3 - SAE

Beacon Interval		Hasil Uji		
100 ms	500 ms	P Value	=	0.983
448	450	Significant	=	Tidak Signifikan
604	603	Mean 100 ms	=	683.8
723	727	Mean 500 ms	=	686
814	818	Perbedaan	=	-2.2
830	832	Kecenderungan	=	Peningkatan

seperti halnya pada uji *open security*, pada WPA versi 3 – SAE menunjukan bahwa *P value* bernilai 0.983 (p>0.05) hal ini berarti H0 diterima dan H1 ditolak atau dapat diartikan bahwa tidak terdapat perbedaan secara signifikan ketika menggunakan nilai *beacon interval* 100 ms dengan 500 ms ketika mengimplementasikan *wireless security protocol* mode WPA versi 3 - SAE, akan tetapi memiliki kecenderungan terjadinya peningkatan yaitu perbedaan antara penggunaan 100 ms dengan 500 ms sebesar 2.2.



Gambar 6. Grafik Penggunaan *Throughput Booster* Pada WPA3-SAE

Tabel 5. Peningkatan *Throughput* Pada *Open Security* dan WPA3-SAE

Beacon Interval	Wireless Security Protocols					
	Open Security			WPA3-SAE		
	128 KB	640 KB	1408 KB	128 KB	640 KB	1408 KB
100 ms	450 Mbps	731 Mbps	848 Mbps	448 Mbps	723 Mbps	830 Mbps
500 ms	452 Mbps	733 Mbps	854 Mbps	450 Mbps	727 Mbps	832 Mbps

Dari tabel 5 terlihat bahwa perubahan nilai *beacon interval* saat menerapkan *wireless security protocols* mode *Open Security* dapat meningkatkan *throughput* hingga 6 Mbps atau 0,7 % saat pengiriman paket 1408 KB dan 4 Mbps atau 0,6 % saat menerapkan mode WPA3-SAE ketika pengiriman paket 640 KB.

2. Pembahasan

Beacon interval adalah jarak waktu pengiriman dari *beacon frames*. Perangkat AP mengirimkan dengan jarak waktu yang regular untuk menentukan posisi user. Pengaturan otomatis pada perangkat yang digunakan adalah 100 milliseconds (ms) atau 1 detik. Pengaturan ini dapat berbeda tergantung perangkat Access Point yang digunakan [12]

Pada penggunaan nilai *beacon interval* yang lebih besar dari nilai *default* dapat mengurangi lalu lintas data yang tidak perlu dalam pemanfaatan saluran jaringan nirkabel, dimana *Access Point* akan mengirimkan *frame beacon* dalam jarak waktu yang lebih panjang untuk memberikan informasi ketersediaan di jaringan, menjaga perangkat tetap terkoneksi dan mendeteksi perangkat baru yang akan terhubung ke jaringan nirkabel sehingga hal ini dapat mengurangi konsumsi energi di *access point* dan meningkatkan ketersediaan *bandwidth*.

Hasil di dalam penelitian ini sama seperti penelitian yang sebelumnya telah dilakukan oleh [6], bagaimana perubahan nilai *beacon interval* lebih besar dari nilai *default* 100 ms dapat meningkatkan *throughput*. Pada penelitiannya peneliti melakukan evaluasi dan perbandingan terhadap penggunaan *beacon interval* 100 ms dengan *beacon interval* 200 ms di dalam komunikasi oportunistik menggunakan teknologi Wi-Fi IEEE 802.11g dalam mode infrastruktur, hasil penelitian menunjukan bahwa penggunaan *beacon interval* 200 ms atau *Double Hundred Interval Beacon* (2HKBI) dapat meningkatkan *throughput* dan pengurangan yang signifikan dalam konsumsi energi.

V. SIMPULAN

Tujuan dari penelitian ini adalah untuk mempelajari penggunaan *beacon interval* dalam meningkatkan kualitas *throughput* ketika mengimplementasikan *wireless security protocol* mode *open security* dan WPA versi 3 – SAE dengan variasi penggunaan di *channel width* 80 Mhz pada jaringan nirkabel standarisasi IEEE 802.11ax dan dari hasil yang telah kami dapatkan maka dapat ditarik kesimpulan bahwa perubahan nilai pada *beacon interval* dengan nilai yang lebih besar dari nilai *default* 100 ms menjadi 500 ms dapat meningkatkan kualitas *throughput* jaringan nirkabel ketika menerapkan *wireless security protocol* baik pada mode *Open Security* maupun WPA versi 3 –SAE, hal ini juga ditunjukan dari hasil *Independent T Test* yang menunjukan kecenderungan meningkat saat menggunakan *beacon interval* 500 ms baik saat menerapkan untuk *open security* maupun WPA versi 3 – SAE.

Peningkatan ini terjadi dikarenakan perangkat *access point* mengurangi konsumsi energi saat *frame beacon* dikirimkan dalam jarak waktu yang lebih panjang untuk memberikan informasi ketersediaan di jaringan kepada pengguna jaringan nirkabel.

Perubahan nilai *beacon interval* saat menerapkan *wireless security protocols* mode *Open Security* dapat meningkatkan *throughput* hingga 0,7 % saat dan 0,6 % saat menerapkan mode WPA3-SAE.

DAFTAR PUSTAKA

[1] A. Siswanto, “Evaluasi Kinerja Wireless 802.11N untuk E Learning,” *IT J. Res. Dev.*, 2017, doi: 10.25299/itjrd.2017.vol1(2).557.

[2] A. Supriyanto, “Analisis Kelemahan Keamanan pada Jaringan Wireless,” *Anal. Keamanan Jar. Wirel.*, 2006.

[3] B. H. I. Saloko Cahyo Saputro, Tri Hargi Saputro, “Analisa Keamanan Jaringan Wireless Menggunakan Metode Wardriving Pada Kampus STMIK MIC Cikarang,” *Pros. Semin.*

Nas. Unimus, vol. 2, no. e-ISSN : 2654-3168, p-ISSN : 2654-3257, pp. 455–461, 2019.

[4] 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.

[5] S. S. Kolahi, S. Narayan, D. D. T. Nguyen, Y. Sunarto, and P. Mani, "The impact of wireless LAN security on performance of different Windows operating systems," *Proc. - IEEE Symp. Comput. Commun.*, pp. 260–264, 2008, doi: 10.1109/ISCC.2008.4625636.

[6] S. Sati and K. Graffi, "Adapting the beacon interval for opportunistic network communications," 2015, doi: 10.1109/ICACCI.2015.7275576.

[7] A. T. Mohammed, "Evaluation of WEP , WPA and WPA2 Security Protocols on 802 . 11ac Client to Server WLAN Performance," no. 9, pp. 1–13, 2016.

[8] T. Pattanasophon, S. Thanee, S. Limpayaraya, T. Kaewkiriya, and A. P. Work, "A Study on Performance of IPv4 , IPv6 on Wireless Network (IEEE 802 . 11ac) with Wireless Security Protocols," vol. 5, no. 1, pp. 5–8, 2017.

[9] S. S. Kolahi and A. A. Almatrook, "Impact of security on bandwidth and latency in IEEE 802.11ac client-to-server WLAN," *Int. Conf. Ubiquitous Futur. Networks, ICUFN*, pp. 893–897, 2017, doi: 10.1109/ICUFN.2017.7993928.

[10] S. Muhammad, J. Zhao, and H. H. Refai, "An Empirical Analysis of IEEE 802.11 ax," no. January, pp. 1–6, 2021, doi: 10.1109/iccspa49915.2021.9385748.

[11] R. Hidayat, "Fitur Utama OFDM dan OFDMA Bagi Jaringan Komunikasi Broadband," *Isu Teknol. STT Mandala*, vol. 5, no. 02, pp. 16–24, 2013.

[12] M. A. Pratama, R. Mayasari, F. T. Elektro, U. Telkom, F. Threshold, and T. Power, "Throughput Analysis Streaming Service on Wireless Lan 802 . 11N," *e-Proceding Eng.*, vol. 4, no. 3, p. 3625, 2017.

[13] C. P. Kohlios and T. Hayajneh, "A comprehensive attack flow model and security analysis for Wi-Fi and WPA3," *Electron.*, 2018, doi: 10.3390/electronics7110284.

[14] E. Lamers, R. Dijksman, A. van der Vegt, M. Sarode, and C. de Laat, "Securing Home Wi-Fi with WPA3 Personal," in *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, Jan. 2021, pp. 1–8, doi: 10.1109/CCNC49032.2021.9369629.

[15] S. Lepaja, A. Maraj, I. Efendiu, and S. Berzati, "The impact of the security mechanisms in the throughput of the WLAN networks," *2018 7th Mediterr. Conf. Embed. Comput. MECO 2018 - Incl. ECYPS 2018, Proc.*, no. February 2020, pp. 1–5, 2018, doi: 10.1109/MECO.2018.8406067.

[16] M. A. Bakri, M. Farhan, and A. Sujatmiko, "Performansi Kinerja Jaringan WLAN 5 GHz Sebagai Alternatif WLAN 2 , 4 GHz pada Area Perkantoran," vol. 7, no. 2, pp. 53–58.

[17] S. S. Kolahi, S. Narayan, D. D. T. Nguyen, and Y. Sunarto, "Performance monitoring of various network traffic generators," 2011, doi: 10.1109/UKSIM.2011.102.

[18] S. S. Kolahi, A. K. Sooran, M. M. U. Khan, and M. F. Nasim, "Performance Comparison of Peer-Peer vs Client-Server 802.11ac WLAN using 80Mhz Channel Size," *Int. J. Comput. Digit. Syst.*, vol. 8, no. 5, pp. 529–534, 2019, doi: 10.12785/ijcds/080511.