Akreditasi Ristekdikti,
No: 30/E/KPT/2019 (Sinta 4)
DOI: https://doi.org/10.31294/p.v23i2.10947

Paradigma,
Vol. 23, No. 2, September 2021
P-ISSN 1410-5063, E-ISSN: 2579-3500

Pengaruh Wireless Security Protocol Pada Throughput Jaringan Wireless 802.11ax

Vian Ardiyansyah Saputro[1], Suwanto Raharjo[2], Eko Pramono[3]

[13]Universitas Amikom Yogyakarta/Magister Teknik Informatika
e-mail: [1]vian.students@amikom.ac.id, [3]eko.p@amikom.ac.id

[2] IST AKPRIND Yogyakarta /Informatika
e-mail: wa2n@akprind.ac.id

Abstrak - Standar dan regulasi untuk teknologi jaringan wireless telah mengalami beberapa perubahan, terbaru IEEE merilis standar baru untuk memperbarui standar jaringan wireless sebelumnya dengan nama IEEE 802.11ax atau yang lebih dikenal dengan Wi-Fi 6. Tidak seperti halnya pada jaringan kabel, di dalam penggunaan jaringan wireless memiliki berbagai permasalahan, salah satunya adalah masalah kerentanan keamanan hal ini dikarenakan penggunaan frekuensi yang sifatnya lebih terbuka dibandingkan dengan menggunakan jaringan berbasis kabel, dengan adanya kerentanan keamanan jaringan wireless tersebut, salah satu cara yang dapat dilakukan untuk mengamankan jaringan wireless adalah dengan mengaktifkan wireless security protocol di perangkat access point yang digunakan, namun cara ini dapat menyebabkan menurunnya kualitas throughput yang di dapatkan oleh pengguna jaringan wireless. Penelitian ini bertujuan untuk membandingkan pengaruh penggunaan wireless security protocol mode WPA2-AES dan WPA3- SAE terhadap throughput jaringan wireless 802.11ax. Hasil penelitian menunjukan bahwa penggunaan wireles security protocol berdampak pada penurunan kualitas throughput jaringan wireless 802.11ax, dimana pada channel width 20 Mhz mengalami penurunan hingga 0.9% baik untuk WPA2-AES maupun WPA3-SAE dan di channel width 40 Mhz mengalami penurunan hingga 1.79% untuk WPA2-AES namun untuk WPA3-SAE kualitas throughput dapat terjaga serta di channel width 80 Mhz mengalami penurunan hingga 1.48% untuk WPA2-AES dan 9.50% untuk WPA3-SAE.

Kata Kunci: 802.11ax, throughput, channel width, wpa2-aes, wpa3-sae

Abstract *- Standards and regulations for wireless network technology have undergone several changes, the latest IEEE released a new standard to update the previous wireless network standard with the name IEEE 802.11ax or better known as Wi-Fi 6. Unlike wired networks, in the use of wireless networks has various problems, one of which is the problem of security vulnerabilities this is due to the use of frequencies that are more open than using a cable-based network, with the security vulnerability of the wireless network, one way that can be done to secure a wireless network is to activate the wireless security protocol. on the access point device used, but this method can cause a decrease in the quality of throughput that is obtained by wireless network users. This study aims to compare the effect of using WPA2-AES and WPA3-SAE wireless security protocol modes on 802.11ax wireless network throughput. The results show that the use of wireless security protocols has an impact on the quality of 802.11ax wireless network throughput, where the 20 Mhz channel width has decreased up to 0.9% for both WPA2-AES and WPA3-SAE and the 40 Mhz channel width has decreased up to 1.79% for WPA2-AES but for WPA3-SAE the throughput quality can be maintained and at 80 Mhz channel width it has decreased by 1.48% for WPA2-AES and 9.50% for WPA3-SAE.*

Keywords: 802.11ax, throughput, channel width, wpa2-aes, wpa3-sae

PENDAHULUAN

Dalam perkembangan jaringan wireless 802.11, standar dan regulasi untuk teknologi jaringan *wireless* telah mengalami beberapa perubahan, terbaru IEEE merilis standar baru untuk memperbarui standar jaringan *wireless* sebelumnya dengan nama IEEE 802.11ax atau yang lebih dikenal

Naskah diterima: 2021-07-12, direvisi: 2021-07-27, disetujui: 2021-07-28

dengan Wi-Fi 6. Seperti kebanyakan teknologi *wireless* baru lainnya, teknologi *wireless* baru ini menawarkan *data rate* hingga 9,6 Gbps dengan menggunakan *channel width* 160 Mhz, dan bekerja di frekuensi 2,4 Ghz dan 5 Ghz, kemudian adanya fitur protokol keamanan baru WPA3 - SAE dimana di dalam protokol keamanan ini menambahkan beberapa fitur baru yang diyakini dapat menyederhanakan keamanan, autentikasi yang lebih kuat, dan meningkatkan keamanan lalu lintas data yang melewati di jaringan tersebut.

Tidak seperti halnya pada jaringan kabel, di dalam penggunaan jaringan *wireless* memiliki berbagai permasalahan, salah satunya adalah masalah kerentanan keamanan hal ini dikarenakan penggunaan frekuensi yang sifatnya lebih terbuka dibandingkan dengan menggunakan jaringan berbasis kabel (Riyan Feraldi., 2019). Secara garis besar, kerentanan keamanan pada jaringan wireless terdiri atas empat layer di mana keempat lapis (layer) tersebut sebenarnya merupakan proses dari terjadinya komunikasi data pada media jaringan *wireless*. Keempat layer tersebut adalah *physical layer, network layer, user layer* dan *application layer* (Supriyanto, 2006).

Dengan adanya kerentanan keamanan jaringan *wireless* seperti diatas, salah satu cara yang dapat dilakukan untuk mengamankan jaringan *wireless* adalah dengan mengaktifkan *wireless security protocol* di perangkat *access point* yang digunakan, namun cara ini dapat menyebabkan menurunnya kualitas *throughput* yang di dapatkan oleh pengguna jaringan *wireless* (Mohammed, 2016).

Berdasarkan penelitian yang dilakukan oleh (Tsetse et al., 2018), mengenai dampak penggunaan *wireless security protocol* pada jaringan *wireless* IEEE 802.11ac dengan menggunakan tiga mode keamanan yang berbeda yaitu mode *no security, personal security*, dan *enterprise security*. Hasilnya menunjukkan bahwa kualitas *throughput* mengalami penurunan berkisar antara 1,6% hingga 8,2% berdasarkan penggunaan pada *protocol transport* (TCP / UDP) dan IP Address (IPV4 / IPv6). Namun pada penelitian yang telah dilakukan hanya dengan menggunakan parameter keamanan mode WPA2 / AES dan server RADIUS. Selanjutnya di dalam penelitian yang dilakukan oleh (Kolahi & Almatrook, 2017) mengenai dampak penggunaan *wireless security protocol* dengan menggunakan mode WPA2 pada jaringan wireless IEEE 802.11ac dengan skenario percobaan *client server*. Hasil penelitian menunjukkan bahwa penurunan kualitas *throughput* berkisar antara 10,22% hingga 18,07% berdasarkan penggunaan pada *transport* protokol (TCP / UDP) dan IP Address (IPV4 / IPv6). Namun di dalam penelitian tersebut hanya menggunakan parameter *wireless security protocol* dengan mode WEP dan WPA.

Selanjutnya pada penelitian mengenai fitur kemanan baru WPA3 yang dilakukan oleh (Kohlios & Hayajneh, 2018), mode keamanan WPA3 menawarkan skema baru yang lebih baik bila dibandingkan dengan mode keamanan WPA2, seperti adanya perbaikan masalah *re-authentication*, *off-line dictionary attacks* dan the KRACK *vulnerability*. Dan adanya fitur *protected management frame (PMF)* yang dapat memberikan pencegahan terhadap serangan DoS (*Denial of Service*) di jaringan *wireless* (Kwon & Choi, 2021). Di dalam metode *password authenticated key exchange*, WPA3 menggunakan protokol SAE (*Simultaneous Authentication of Equals*) yang dirancang untuk menggantikan autentikasi WPA2 – PSK dan mendukung autentikasi P2P (*Peer to Peer*) (Sun, 2019).

Sehingga berdasarkan literatur penelitian tersebut maka perlu dilakukan penelitian dengan menggunakan *wireless security protocol* mode WPA2 - AES dan mode WPA3 – SAE sebagai mode terbaru di dalam keamanan jaringan *wireless* dan juga penggunaan variasi *channel width* 20 Mhz, 40 Mhz dan 80 Mhz.

Tujuan dari penelitian ini adalah untuk membandingkan pengaruh penggunaan *wireless security protocol* mode WPA2-AES dan WPA3-SAE terhadap *throughput* jaringan *wireless* 802.11ax yang dapat menghasilkan kualitas *throughput* tinggi untuk penggunaan di *channel width* 20 Mhz, 40 Mhz dan 80 Mhz. Metode penelitian yang dilakukan adalah dengan mengacu pada penelitian yang telah dilakukan oleh (Mohammed, 2016), sehingga nantinya penggunaan *wireless security protocol* lebih maksimal dan menjadi tolak ukur kinerja jaringan di lingkungan *wireless* IEEE 802.11ax.

Untuk penelitian yang kami lakukan dapat memberikan kontribusi ilmu pengetahuan mengenai bagaimana penggunaan *wireless security protocol* memberikan pengaruh terhadap *throughput* jaringan *wireless* IEEE 802.11ax, hal ini dikarenakan beberapa penelitian lain yang sudah dilakukan, sebagian besar penelitian dilakukan dengan standar IEEE 802.11 sebelumnya.

METODOLOGI PENELITIAN

Metode penelitian yang digunakan adalah eksperimental yaitu membuat suatu eksperimen untuk mendapatkan hasil dan selanjutnya hasil tersebut dianalisis. Di dalam penelitian ini terbagi menjadi 4 tahapan penelitian seperti yang terlihat di dalam gambar 1.

Sumber : (Saputro et al., 2021)

Gambar 1. Tahapan penelitian

Gambar 1 adalah tahapan penelitian, berikut adah penjelasan setiap tahapan yang ada di dalam gambar tersebut :

1. Perancangan Topologi

Di dalam perancangan topologi, skenario topologi jaringan menggunakan topologi *client server* dimana di dalam percobaan ini akan menggunakan PC *client* yang terinstal sistem operasi Windows 10 Pro dan terpasang *wireless card* TPLink AX3000 yang nantinya terhubung ke jaringan *wireless* menggunakan *access point indoor* TPLink Archer AX1500, sedangkan untuk PC *server* terinstal sistem operasi Windows Server 2016 *Standard* (GUI) yang terhubung ke *access point* menggunakan kabel UTP Cat6. Di dalam penelitian ini, akan dilakukan dengan menggunakan frekuensi 5 Ghz yang dapat menghasilkan kualitas *throughput* lebih tinggi dibandingkan dengan penggunaan frekuensi 2.4 GHz (Lepaja et al., 2018) serta frekuensi 5 Ghz dapat menjadi alternatif digunakan di dalam jaringan *wireless* untuk menunjang pekerjaan perkantoran dengan aktifitas seperti *browsing* internet, *download*, pertukaran data, dan *video conference* (Bakri et al., n.d.), sehingga nantinya di dapatkan hasil kualitas *troughput* maksimal jaringan *wireless* IEEE 802.11ax. Jarak antara PC *client* dengan *access point indoor* adalah 1 meter hal ini untuk mempertahankan kekuatan sinyal yang optimal seperti ditunjukan di dalam gambar 2.

Sumber : (Saputro et al., 2021)

Gambar 2. Skenario Topologi Pengujian

Di dalam perancangan topologi pengujian menggunakan IP address versi 4 untuk setiap perangkat yang terhubung di dalam skenario jaringan diatas, dimana PC *server* menggunakan IP *Address* 192.168.0.1/24, dan untuk PC *client* menggunakan IP Address 192.168.0.2/24 serta *access Point* TPLink AX1500 yang berfungsi sebagai penghubung antara PC *server* dan PC *client* menggunakan IP *Address* 192.168.0.254/24. Selanjutnya, berbagai parameter pengujian diterapkan meliputi penggunaan *wireless security protocol*, dan jenis paket TCP *Window Size*. Parameter yang digunakan untuk pengujian dirangkum dalam tabel 1.

Tabel 1. Parameter Pengujian

Parameter	
Security Protocols	*Open Security*, WPA2 – AES, WPA3 - SAE
Network Traffic	TCP
Window Size	128KB, 384KB, 640KB, 1152KB, 1408KB

Sumber : (Saputro et al., 2021)

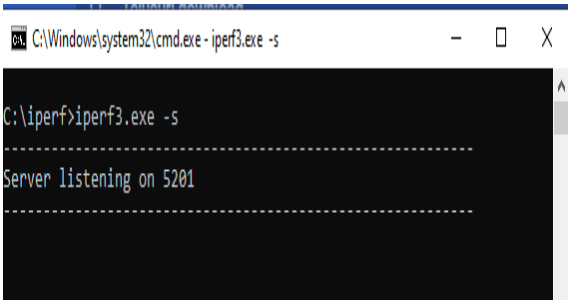
Untuk mendapatkan hasil yang maksimal di dalam penelitian ini, maka kami mempertimbangkan penggunaan perangkat keras untuk PC *Server*, PC *Client*, *Access Point* dan *Wireless Card Adapter* dengan spesifikasi sebagai berikut :

Tabel 2. Spesifikasi Perangkat Keras

Perangkat Keras	**Fungsi**	**Spesifikasi**
TP-Link Archer AX10 AX1500 Wireless Dual-Band Gigabit Router	*Wireless Access Point*	Wi-Fi 6 (802.11ax) with Up to 1501 Mb/s, 2.4 GHz / 5 GHz (Dual-Band), Support Gigabit LAN Ports, Support WPA3 SAE.
TP-LinkAX3000 WiFi Card	*Wireless Card Adapter*	WiFi 6 PCIe Card, Up to 2400Mbps, 802.11AX Dual Band Wireless.
Server	*PC Server*	Intel Xeon E-2224G 3.5GHz, 8GB DDR4, 1TB SATA 3.5in, D-LINK Gigabit Ethernet Adapter DGE-560T.
Client	*PC Client*	Intel Core i9-10900 2.8Ghz, DDR4 32 GB (Single Channel), SSD 128 GB

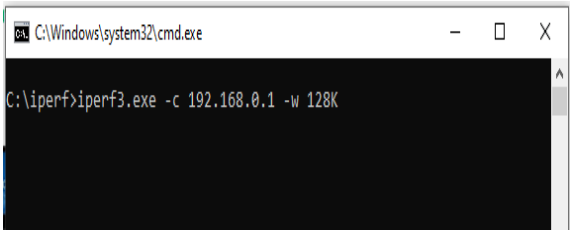
Sumber : (Saputro et al., 2021)

Penggunaan aplikasi *iperf* yang terinstal di PC *client* sebagai *transmitter* dan di PC server sebagai *receiver* berfungsi untuk menguji *throughput* yang dihasilkan oleh jaringan *wireless* 802.11ax. Dimana perintah untuk menjalankan aplikasi *iperf* menggunakan *command prompt* Microsoft Windows, berikut perintah konfigurasi yang digunakan :



Sumber : (Saputro et al., 2021)

Gambar 3. Perintah iperf untuk PC *server* yang bertindak sebagai *receiver*

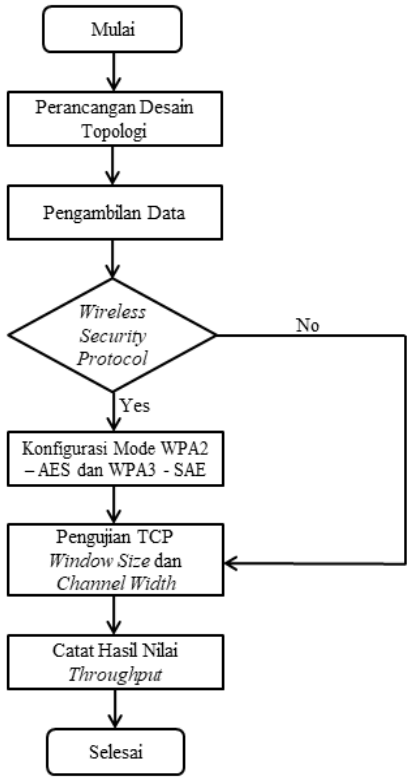


Sumber : (Saputro et al., 2021)

Gambar 4. Perintah iperf untuk PC *client* yang bertindak sebagai *transmitter*

2. Skenario Pengujian

Penggunaan skenario pengujian di dalam penelitian ini bertujuan untuk mendapatkan nilai *throughput* tertinggi dari penggunaan *No security*, WPA2-AES dan WPA3-SAE dengan variasi penggunaan *channel width* 20 Mhz, 40 Mhz dan 80 Mhz. Konseptual skenario pengujian terlihat di kerangka penelitian di dalam gambar 5.



Sumber : (Saputro et al., 2021)

Gambar 5. Kerangka Penelitian

Gambar 5 merupakan kerangka konseptual penelitian yang dilakukan peneliti pada penelitian ini. Berikut penjelasan dari setiap langkah yang dilakukan:

a. Perancangan Topologi : Melakukan perancangan desain topologi untuk penelitian ini dengan tujuan untuk mendapatkan hasil pengujian sesuai dengan tujuan penelitian.
b. Pengambilan Data Skenario Pertama: Melakukan pengambilan data dimana di dalam skenario pertama ini *access point* menggunakan *channel width* 20 Mhz dan *wireless security protocol No Security*, WPA2-AES dan WPA3-SAE. selanjutnya pengujian menggunakan aplikasi *iperf* dengan mengirimkan paket data berupa paket TCP *Window Size* dengan ukuran 128KB, 384KB, 640KB, 1152KB, dan 1408KB dari PC *client* ke PC *Server* yang terhubung menggunakan *access point*. Percobaan pengiriman paket data dari PC *client* menuju PC *server* melalui jaringan *wireless* akan dilakukan sebanyak 10 kali dimana setiap pengujian sebanyak 10 detik.
c. Pengambilan Data Skenario Kedua: Melakukan pengambilan data dimana di dalam skenario kedua ini *access point* menggunakan *channel width* 40 Mhz dan penggunaan *wireless security protocols No Security*, WPA2-AES dan WPA3-SAE. selanjutnya pengujian menggunakan aplikasi *iperf* dengan mengirimkan paket data berupa paket TCP *Window Size* dengan ukuran 128KB, 384KB, 640KB, 1152KB, dan 1408KB dari PC *client* ke PC *Server* yang terhubung menggunakan *access point*. Percobaan pengiriman paket data dari PC *client* menuju PC *server* melalui jaringan *wireless* akan dilakukan sebanyak 10 kali dimana setiap pengujian sebanyak 10 detik.
d. Pengambilan Data Skenario Ketiga: Melakukan pengambilan data dimana di dalam skenario kedua ini *access point* menggunakan *channel width* 80 Mhz dan penggunaan *wireless security protocols No Security*, WPA2-AES dan WPA3-SAE. selanjutnya pengujian menggunakan aplikasi *iperf* dengan mengirimkan paket data berupa paket TCP *Window Size* dengan ukuran 128KB, 384KB, 640KB, 1152KB, dan 1408KB dari PC *client* ke PC *Server* yang terhubung menggunakan *access point*. Percobaan pengiriman paket data dari PC *client* menuju PC *server* melalui jaringan *wireless* akan dilakukan sebanyak 10 kali dimana setiap pengujian sebanyak 10 detik.

3. Analisa Hasil Pengujian

Analisa hasil pengujian dilakukan untuk mengetahui nilai *throughput* yang dihasilkan terhadap pengaruh penggunaan *wireless security protocol*. Hasil pengujian disajikan ke dalam bentuk grafik *line*

untuk melihat naik dan turunnya data hasil pengujian yang telah didapatkan.

4. Pembuatan Laporan

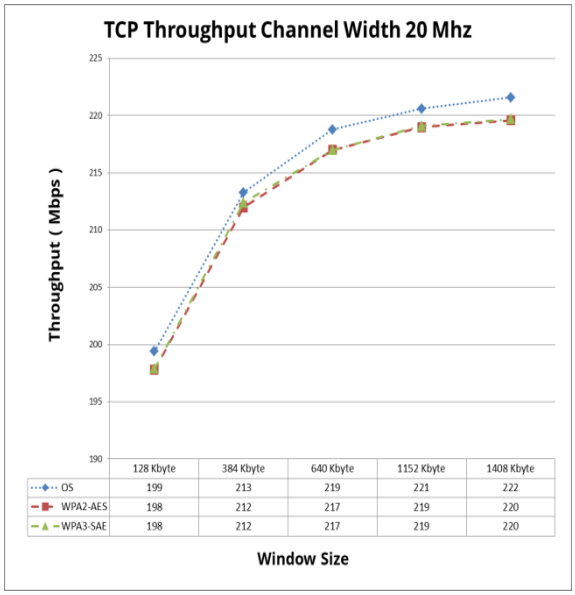
Pembuatan laporan bertujuan untuk merangkum semua hal yang berkaitan dengan penelitian ini seperti studi literatur yang digunakan, metode penelitian yang digunakan, skenario perancangan desain jaringan, skenario pengujian, hasil dan pembahasan pengujian.

HASIL DAN PEMBAHASAN

Pengujian ini dilakukan untuk mengetahui nilai *throughput* yang dihasilkan dengan variasi pengujian dengan mengirimkan paket TCP *Window Size* ukuran 128 KB, 384 KB, 640 KB, 1152 KB, dan 1408 KB dari PC *Client* menuju PC *Server* yang terhubung dengan *Access Point*. Dimana terdapat 3 skenario penggunaan *wireless security protocol* yaitu *Access Point* menggunakan mode *open security*, WPA2-AES dan WPA3-SAE.

Berikut hasil dan pembahasan dari pengujian yang telah dilakukan :

1. Perbandingan Penggunaan *Wireless Security Protocol* Untuk *Channel Width* 20 Mhz



Sumber : (Saputro et al., 2021)

Gambar 6. Grafik Perbandingan *Throughput* untuk *Channel Width* 20 Mhz

Berdasarkan gambar 6, menunjukan bahwa pada penggunaan *wireless security protocols* WPA2-AES maupun WPA3 – SAE di *channel width* 20 Mhz, *throughput* mengalami penurunan bila dibandingkan ketika jaringan *wireless* tidak menerapkan *wireless security* (*No Security*), dimana penggunaan WPA2-AES dan WPA3-SAE ketika pengujian dengan mengirimkan paket TCP *window size* dengan ukuran 128 Kbyte dan 384 Kbyte mengalami penurunan *throughput* sebanyak 1 Mbps atau 0.5%. *Throughput* mengalami penurunan kembali ketika pengujian WPA2-AES dan WPA3-SAE menggunakan ukuran TCP *window size* lebih besar yaitu menggunakan ukuran TCP *window size* berukuran 640 Kbyte, 1152 Kbyte dan 1408 Kbyte mengalami penurunan sebanyak 2 Mbps atau 0.9%.

Hasil pengujian terlihat di dalam tabel 3.

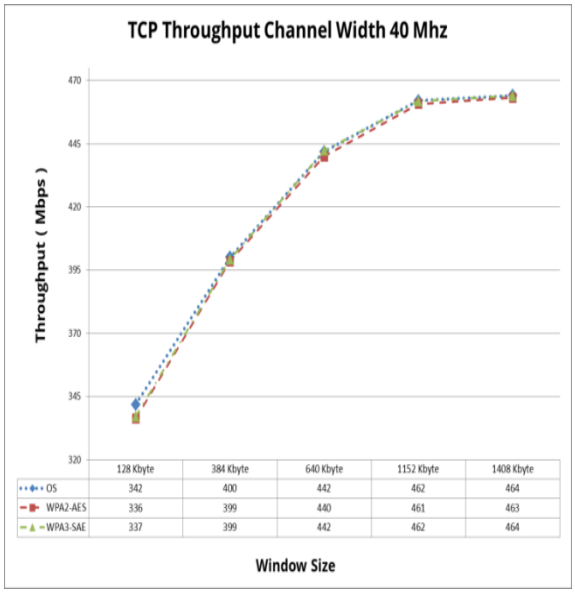
Tabel 3. Persentase Penurunan *Wireless Security Protocol* di *Channel Width* 20 Mhz

Wireless Security Protocols	Ukuran Window Size (KByte)				
	128	384	640	1152	1408
WPA2 - AES	0.5%	0.5%	0.9%	0.9%	0.9%
WPA3 - SAE	0.5%	0.5%	0.9%	0.9%	0.9%

Sumber : (Saputro et al., 2021)

Dari tabel 3, terlihat bahwa untuk *channel width* 20 Mhz jaringan *wireless* 802.11ax semakin besar ukuran TCP *window Size* maka *throughput* yang didapatkan oleh PC *client* akan mengalami penurunan semakin besar.

2. Perbandingan Penggunaan *Wireless Security Protocol* Untuk *Channel Width* 40 Mhz



Sumber : (Saputro et al., 2021)

Gambar 7. Grafik Perbandingan *Throughput* untuk *Channel Width* 40 Mhz

Berdasarkan gambar 7, menunjukan bahwa penggunaan *wireless security protocols* WPA2-AES dan WPA3 – SAE di *channel width* 40 Mhz, *throughput* juga mengalami penurunan signifikan. Ketika jaringan *wireless* menerapkan WPA2-AES dan pengujian menggunakan TCP *Window Size* dengan ukuran 128 Kbyte, *throughput* mengalami penurunan sebanyak 6 Mbps atau 1.79% sedangkan penerapan WPA3-SAE, *throughput* mengalami penurunan sebanyak 5 Mbps atau 1.48%. Hasil pengujian selanjutnya untuk WPA2-AES ketika menggunakan ukuran TCP *window Size* 384 Kbyte, 1152 Kbyte dan 1408 Kbyte *throughput* mengalami

penurunan sebanyak 1 Mbps atau 0.25% dan 2 Mbps atau 0.45% ketika menggunakan ukuran TCP *windows size* 640 Kbyte. Untuk penggunaan WPA3-SAE, *troughput* mengalami penurunan kembali ketika pengujian menggunakan ukuran TCP *window size* 384 Kbyte sebanyak 1 Mbps atau 0.25%, selanjutnya *throughput* yang di dapatkan PC *client* tidak mengalami penurunan walaupun menerapkan mode WPA3-SAE ketika pengujian menggunakan ukuran TCP *window size* 640 Kbyte, 1152 Kbyte dan 1408 Kbyte. Hasil pengujian terlihat di dalam tabel 4.

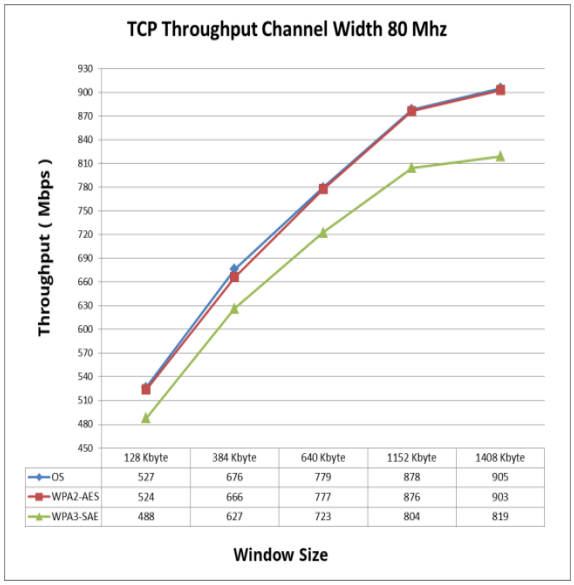
Tabel 4. Persentase Penurunan *Wireless Security Protocol* di *Channel Width* 40 Mhz

Wireless Security Protocols	Ukuran Window Size (KByte)				
	128	384	640	1152	1408
WPA2 - AES	1.79%	0.25%	0.45%	0.25%	0.25%
WPA3 - SAE	1.48%	0.25%	0%	0%	0%

Sumber : (Saputro et al., 2021)

Dari tabel 4, terlihat bahwa untuk *channel width* 40 Mhz jaringan *wireless* 802.11ax penggunaan WPA2-AES mengalami presentase penurunan paling signifikan hingga 1.79% bila dibandingkan dengan WPA3-SAE. Dimana *throughput* yang di dapatkan PC *client* ketika menerapkan WPA3-SAE sama seperti ketika tidak menerapkan *wireless security* (No Security), hal ini ditunjukan ketika pengujian pengiriman paket menggunakan ukuran TCP *window size* 640 Kbyte, 1152 Kbyte dan 1408 Kbyte.

3. Perbandingan Penggunaan *Wireless Security Protocol* Untuk *Channel Width* 80 Mhz



Sumber : (Saputro et al., 2021)

Gambar 8. Grafik Perbandingan *Throughput* untuk *Channel Width* 80 Mhz

Berdasarkan gambar 8, penerapan *wireless security protocol* di *channel width* 80 Mhz menunjukan bahwa penggunaan WPA2-AES menurunkan *throughput* hingga 1.48% atau sebanyak 10 Mbps ketika pengujian menggunakan ukuran TCP *window size* 384 Kbyte, namun ketika pengujian menggunakan ukuran TCP *window size* lebih besar yaitu 640 Kbyte, 1152 Kbyte dan 1408 Kbyte penurunan *throughput* lebih sedikit hanya 1 – 2 Mbps atau 0.22% - 0.26%. Berbeda dengan WPA2-AES, hasil pengujian untuk WPA3-SAE menunjukan *throughput* yang didapatkan PC *client* mengalami penurunan sangat besar hingga 86 Mbps atau 9.50% ketika pengujian menggunakan ukuran TCP *window size* 1408 Kbyte. seperti yang ditunjukan di dalam tabel 5.

Tabel 5. Persentase Penurunan *Wireless Security Protocol* di *Channel Width* 80 Mhz

Wireless Security Protocols	Ukuran Window Size (Kbyte)				
	128	384	640	1152	1408
WPA2 - AES	0.57%	1.48%	0.26%	0.23%	0.22%
WPA3 - SAE	7.4%	7.25%	7.19%	8.43%	9.50%

Sumber : (Saputro et al., 2021)

Terlihat di dalam tabel 5 menunjukan bahwa penerapan WPA3-SAE di *channel width* 80 Mhz mengalami penurunan *throughput* seiring penggunaan ukuran TCP *window size* yang semakin besar. Hal ini berbeda ketika penggunaan WPA2 – AES di *channel width* 80 Mhz seiring penggunaan ukuran TCP *window size* yang besar penurunan *throughput* hanya 1 – 2 Mbps atau 0.22% - 0.26%.

KESIMPULAN

Berdasarkan hasil pengujian yang telah dilakukan untuk dampak penggunaan *wireless security protocol* mode *Open Security*, WPA2 – AES dan WPA3 – SAE dengan variasi penggunaan *channel width* 20 Mhz, 40 Mhz dan 80 Mhz pada jaringan *wireless* 802.11ax maka dapat ditarik kesimpulan bahwa penggunaan *wireless security protocol* baik WPA2-AES dan WPA3-SAE di dalam jaringan *wireless* IEEE 802.11ax berdampak pada penurunan kualitas *throughput* yang didapatkan oleh PC *client*.
Selanjutnya untuk hasil skenario pertama pengujian di *channel width* 20 Mhz menunjukan bahwa ketika jaringan *wireless* menggunakan *wireless security protocols* WPA2-AES dan WPA3-SAE semakin besar ukuran TCP *windows size* yang dikirimkan, penurunan *throughput* semakin besar sebanyak 0.9%. dan untuk hasil skenario kedua pengujian di *channel width* 40 Mhz menunjukan bahwa ketika penggunaan WPA2-AES mengalami presentase penurunan paling signifikan hingga 1.79% bila dibandingkan dengan WPA3-SAE hanya 1.48%. Namun penggunaan WPA3-SAE di channel width 40 Mhz menunjukan hasil yang baik terlihat semakin

besar ukuran TCP *window size* ,*throughput* yang di dapatkan sama seperti penggunaan *open security*. Sehingga berdasarkan hasil pengujian untuk penggunaan *wireless security protocol* di *channel width* 40 Mhz dapat menggunakan mode WPA3-SAE kemudian untuk hasil skenario ketiga pengujian di *channel width* 80 Mhz menunjukan bahwa penggunaan WPA2-AES lebih baik karena hanya mengalami penurunan hingga 1.48% bila dibandingkan dengan penggunaan WPA3-SAE yang mengalami penurunan signifikan hingga 9.50%. Sehingga berdasarkan hasil pengujian untuk penggunaan *wireless security protocol* di *channel width* 80 Mhz dapat menggunakan mode WPA2-AES.

Tabel 6. Persentase Penurunan Terbesar Dari Hasil Pengujian

Wireless Security Protocols	Channel Width		
	20 Mhz	40 Mhz	80 Mhz
WPA2 - AES	0.9%	1.79%	1.48%
WPA3 - SAE	0.9%	1.48%	9.50%

Sumber : (Saputro et al., 2021)

REFERENSI

Bakri, M. A., Farhan, M., & Sujatmiko, A. (n.d.). *Performansi Kinerja Jaringan WLAN 5 GHz Sebagai Alternatif WLAN 2 , 4 GHz pada Area Perkantoran*. *7*(2), 53–58.

Kohlios, C. P., & Hayajneh, T. (2018). A comprehensive attack flow model and security analysis for Wi-Fi and WPA3. *Electronics (Switzerland)*. https://doi.org/10.3390/electronics7110284

Kolahi, S. S., & Almatrook, A. A. (2017). Impact of security on bandwidth and latency in IEEE 802.11ac client-to-server WLAN. *International Conference on Ubiquitous and Future Networks, ICUFN*, 893–897. https://doi.org/10.1109/ICUFN.2017.7993928

Kwon, S., & Choi, H. K. (2021). Evolution of Wi-Fi Protected Access: Security Challenges. *IEEE Consumer Electronics Magazine*. https://doi.org/10.1109/MCE.2020.3010778

Lepaja, S., Maraj, A., & Berzati, S. (2018). *Wireless LAN Planning and Performance Analysis*. https://doi.org/10.2507/daaam.scibook.2018.26

Mohammed, A. T. (2016). *Evaluation of WEP , WPA and WPA2 Security Protocols on 802 . 11ac Client to Server WLAN Performance*. *9*, 1–13.

Riyan Feraldi., 2019. (2019). Kelemahan Keamanan Jaringan Wireless. *Journal of Chemical Information and Modeling*.

Saputro, V. A., Raharjo, S., & Pramono, E. (2021). *Pengaruh Wireless Security Protocol Pada Throughput Jaringan Wireless 802.11ax*. *23*(2), 1–7.

Sun, S. (2019). A Chosen Random Value Attack on WPA3 SAE authentication protocol. *Cryptology EPrint Archive*.

Supriyanto, A. (2006). Analisis Kelemahan Keamanan pada Jaringan Wireless. *Analisis Keamanan Jaringan Wireless*.

Tsetse, A., Bonniord, E., Appiah-Kubi, P., & Tweneboah-Kodua, S. (2018). Performance Study of the Impact of Security on 802.11ac Networks. *Advances in Intelligent Systems and Computing*, *738*, 11–17. https://doi.org/10.1007/978-3-319-77028-4_3

PROFIL PENULIS

Vian Ardiyansyah Saputro, Lahir di Kota Pemalang, 29 Maret 1990, Alumni D4 Teknik Telekomunikasi Politeknik Negeri Semarang dan saat ini sedang menempuh pendidikan Magister Teknik Informatika di Universitas AMIKOM Yogyakarta. Saat ini saya bekerja sebagai Senior IT Infrastruktur dna Support di salah satu perusahaan FCMG di Karawang. Silahkan Anda juga dapat mengunjungi website pribadi saya di www.acavicomputech.com