TESIS

ANALISIS DAMPAK PENGGUNAAN WIRELESS SECURITY PROTOCOL (OPEN SECURITY, WPA2 - AES DAN WPA3 - SAE) TERHADAP KUALITAS THROUGHPUT JARINGAN WIRELESS IEEE 802.11AX

Disusun oleh:

Nama : **Vian Ardiyansyah Saputro**
NIM : **20.77.1258**
Konsentrasi : **Informatics Technopreneurship**

PROGRAM STUDI S2 TEKNIK INFORMATIKA

PROGRAM PASCASARJANA UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2020

TESIS

ANALISIS DAMPAK PENGGUNAAN WIRELESS SECURITY PROTOCOL (OPEN SECURITY, WPA2 - AES DAN WPA3 - SAE) TERHADAP KUALITAS THROUGHPUT JARINGAN WIRELESS IEEE 802.11AX

ANALYSIS OF THE IMPACT OF THE USE OF WIRELESS SECURITY PROTOCOL (OPEN SECURITY, WPA2-AES DAN WPA3-SAE) ON THE QUALITY OF THROUGHPUT NETWORK OF IEEE 802.11AX WIRELESS NETWORK

Diajukan untuk memenuhi salah satu syarat memperoleh derajat Magister

Disusun oleh:

Nama	**: Vian Ardiyansyah Saputro**
NIM	**: 20.77.1258**
Konsentrasi	**: Informatics Technopreneurship**

PROGRAM STUDI S2 TEKNIK INFORMATIKA

PROGRAM PASCASARJANA UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2020

HALAMAN PENGESAHAN

ANALISIS DAMPAK PENGGUNAAN WIRELESS SECURITY PROTOCOL (OPEN SECURITY, WPA2 - AES DAN WPA3 - SAE) TERHADAP KUALITAS THROUGHPUT JARINGAN WIRELESS IEEE 802.11AX

ANALYSIS OF THE IMPACT OF THE USE OF WIRELESS SECURITY PROTOCOL (OPEN SECURITY, WPA2-AES DAN WPA3-SAE) ON THE QUALITY OF THROUGHPUT NETWORK OF IEEE 802.11AX WIRELESS NETWORK

Dipersiapkan dan Disusun oleh

Vian Ardiyansyah Saputro

20.77.1258

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tesis
Program Studi S2 Teknik Informatika
Program Pascasarjana Universitas AMIKOM Yogyakarta
pada hari Selasa, 1 Maret 2022

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer

Yogyakarta, 1 Maret 2022
Rektor

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

HALAMAN PERSETUJUAN

ANALISIS DAMPAK PENGGUNAAN WIRELESS SECURITY PROTOCOL (OPEN SECURITY, WPA2 - AES DAN WPA3 - SAE) TERHADAP KUALITAS THROUGHPUT JARINGAN WIRELESS IEEE 802.11AX

ANALYSIS OF THE IMPACT OF THE USE OF WIRELESS SECURITY PROTOCOL (OPEN SECURITY, WPA2-AES DAN WPA3-SAE) ON THE QUALITY OF THROUGHPUT NETWORK OF IEEE 802.11AX WIRELESS NETWORK

Dipersiapkan dan Disusun oleh

Vian Ardiyansyah Saputro

20.77.1258

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tesis
Program Studi S2 Teknik Informatika
Program Pascasarjana Universitas AMIKOM Yogyakarta
pada hari Selasa, 1 Maret 2022

Pembimbing Utama	**Anggota Tim Penguji**
Dr. Suwanto Raharjo, S.Si.,M.Kom	**Dr. Andi Sunyoto, M.Kom**
NIK. 999106	**NIK. 190302036**
	Alva Hendi Muhammad, S.T., M.Eng., Ph.D.
Pembimbing Pendamping	**NIK. 190302493**
Eko Pramono, S.Si., M.T	**Dr. Suwanto Raharjo, S.Si.,M.Kom**
NIK. 555006	**NIK. 999106**

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer

Yogyakarta, 1 Maret 2022
Direktur Program Pascasarjana

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN TESIS

Yang bertandatangan di bawah ini,

Nama mahasiswa : Vian Ardiyansyah Saputro
NIM : 20.77.1258
Konsentrasi : Informatics Technoprenecurship

Menyatakan bahwa Tesis dengan judul berikut:
Analisis Dampak Penggunaan Wireless Security Protocol (Open Security, WPA2 - AES Dan WPA3 - SAE) Terhadap Kualitas Throughput Jaringan Wireless IEEE 802.11AX

Dosen Pembimbing Utama : Dr. Suwanto Raharjo, S.Si.,M.Kom
Dosen Pembimbing Pendamping : Eko Pramono, S.Si., M.T

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim Dosen Pembimbing
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi

Bekasi, 1 Maret 2022
Yang Menyatakan,

Vian Ardiyansyah Saputro

HALAMAN PERSEMBAHAN

Dengan segala puji syukur kepada Allah SWT yang telah memberikan Rahmat dan Hidayah-Nya dan atas dukungan serta doa dari orang-orang tercinta, akhirnya tesis ini dapat terselesaikan dengan baik. Oleh karena itu, dengan rasa bangga dan bahagia, tesis ini saya persembahkan kepada:

1. Ibunda Miji Wuryani, Ibunda Marwati dan Istri Ady Ari Wahyu Ningsih tercinta yang telah memberikan dukungan moril maupun materi serta doa yang tiada henti, motivasi dan kesabaran kepada saya.
2. Bapak Dr. Suwanto Raharjo, S.Si., M.Kom dan Bapak Eko Pramono, S.Si., M.T selaku dosen pembimbing yang selalu memberikan arahan dan bimbingan positif dalam menyelesaikan Tesis ini hingga tesis ini dapat terselesaikan dengan baik.
3. Acavi Computech Cikarang yang telah memperbolehkan kami untuk melakukan penelitian bersama.
4. Sahabat seperjuangan Angkatan ketiga PJJ Universitas Amikom Yogyakarta yang selalu menemani dari awal semester satu hingga pengerjaan Tesis ini selesai dan selalu memberikan semangat untuk tidak menyerah.
5. Segenap keluarga Admisi MTI Universitas Amikom, yang selalu sabar dengan kami semua hingga Tesis kami akhirnya selesai. Serta semua pihak yang telah membantu serta mendukung saya yang tidak bisa saya sebutkan satu persatu.

Saya ucapkan terima kasih, baik teman-teman yang saya tulis maupun tidak bisa saya tulis, segala doa yang baik untuk teman-teman semua. Semoga Tesis ini dapat bermanfaat dan berguna di masa yang akan datang. Amiiin.

HALAMAN MOTTO

"Sesungguhnya sesudah kesulitan itu ada kemudahan, maka apabila kamu telah selesai dari suatu urusan, kerjakanlah dengan sungguh-sungguh urusan yang lain, dan hanya kepada Tuhanmulah hendaknya kamu berharap"

(Q.S Al-Insyirah : 6-8)

"Setiap fase yang kamu jalani harus bisa mendatangkan pelajaran untuk naik ke fase berikutnya."

-Merry Riana-

"Semua kehidupan adalah eksperimen. Semakin banyak eksperimen yang kamu lakukan, semakin baik."

-Ralph Waldo Emerson-

KATA PENGANTAR

Puji syukur kita panjatkan kepada Allah SWT atas Karunia- Nya sehingga penulis dapat menyelesaikan Tesis dengan judul "Analisis Dampak Penggunaan *Wireless Security Protocol* (Open Security, WPA2 - AES Dan WPA3 - SAE) Terhadap Kualitas *Throughput* Jaringan *Wireless* IEEE 802.11AX" dapat terselesaikan dengan baik. Kritik dan saran sangat diharapkan penulis agar dapat lebih baik lagi di kemudian hari.

Dalam penyusunan dan penulisan tesis ini tidak terlepas dari bantuan dan bimbingan serta dukungan dari berbagai pihak. Oleh karena itu dalam kesempatan ini penulis dengan senang hati menyampaikan terima kasih kepada:

1. Prof. Dr. M. Suyanto, M.M. selaku rektor Universitas AMIKOM Yogyakarta.
2. Prof. Dr. Kusrini, M.Kom. selaku Direktur Program Pascasarjana Universitas AMIKOM Yogyakarta yang telah menunjuk dosen pembimbing sehingga memperlancar penulis dalam menyelesaikan tesis.
3. Dr. Suwanto Raharjo, S.Si., M.Kom dan Bapak Eko Pramono, S.Si., M.T, selaku pembimbing utama dan pendamping yang telah mencurahkan perhatian, bimbingan, nasihat, doa, dan kepercayaan yang sangat berarti bagi penulis serta telah meluangkan waktu dalam memberikan arahan dan masukan selama penelitian dan penyusunan tesis.
4. Orang tua dan Istri tercinta yang telah memberikan doa dan motivasi sehingga menjadi penyemangat bagi penulis dalam mengerjakan tesis.

6. Teman-teman seperjuangan yang telah memberikan semangat dan dukungan selama masa pendidikan hingga tesis ini dapat terselesaikan dengan baik.
7. Semua pihak yang telah membantu, baik secara langsung maupun tidak langsung yang tidak dapat penulis sebutkan satu per satu.

Akhir kata, semoga tesis ini bermanfaat, khususnya bagi penulis dan umumnya bagi masyarakat dalam rangka menambah wawasan pengetahuan.

Bekasi, 19 Februari 2021

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

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 penerapan *wireless security protocol* dengan mode WPA2 – AES lebih baik dibandingkan dengan WPA3-SAE untuk penggunaan di *channel width* 20 Mhz, dan untuk penggunaan di *channel width* 40 Mhz penggunaan mode WPA3-SAE lebih baik dibandingkan dengan WPA2-AES begitu juga untuk

penggunaan di *channel width* 80 Mhz penggunaan mode WPA3-SAE lebih baik dibandingkan dengan WPA2-AES. Selanjutnya perubahan nilai pada *beacon interval* dengan nilai yang lebih besar dapat meningkatkan kualitas *throughput* jaringan *wireless* ketika menerapkan *wireless security protocol* baik di *channel width* 20 Mhz, 40 Mhz dan 80 Mhz.

Kata kunci: 802.11ax, throughput,wpa2-aes, wpa3-sae,beacon interval

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 the 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 the wireless security protocol has an impact on the quality of the 802.11ax wireless network throughput, where the application of the wireless security protocol with WPA2 - AES mode is better than WPA3-SAE for use in channel width 20 Mhz, and for use in channel width. 40 Mhz WPA3-SAE mode usage is better than WPA2-AES as well as 80 Mhz channel width usage WPA3-SAE mode is better than WPA2-AES. Furthermore, changing the value of the beacon interval with a larger value can improve the quality of wireless network throughput when implementing wireless security protocols in channel widths of 20 Mhz, 40 Mhz and 80 Mhz.

Keyword: 802.11ax, throughput,wpa2-aes, wpa3-sae,beacon interval

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Teknologi *wireless local area network* (WLAN) merupakan teknologi yang dapat digunakan untuk memindahkan data dari satu perangkat ke perangkat lainnya tanpa menggunakan media transmisi kabel dengan memanfaatkan gelombang radio. Meskipun kehadiran teknologi ini tidak menggantikan peran jaringan kabel secara keseluruhan, namun sejak kehadiran teknologi ini telah memudahkan penggunanya untuk terkoneksi ke jaringan global. 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 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 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 dimana 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 didapatkan oleh pengguna jaringan *wireless* (Mohammed, 2016).

Berdasarkan penelitian yang dilakukan oleh (Tsetse et al., 2018), penulis telah menganalisis bagaimana dampak penggunaan *wireless security protocol* pada jaringan *wireless* IEEE 802.11ac dengan menggunakan tiga mode keamanan yang berbeda yaitu mode *open 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) penulis melakukan analisa terhadap 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 pada penelitian ini belum memasukkan parameter *wireless security protocol* keamanan lain seperti WEP dan WPA.

Sehingga berdasarkan literatur penelitian sebelumnya maka akan dilakukan penelitian dengan menggunakan standar jaringan *wireless* terbaru IEEE 802.11ax dan menggabungkan parameter yang digunakan dalam penelitian sebelumnya seperti menggunakan *wireless security protocol* mode *Open Security*, WPA2 dengan enkripsi 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 serta penggunaan parameter *beacon interval*.

Tujuan dari penelitian ini adalah untuk mencari mode *wireless security protocol* manakah yang baik diantara WPA2 dengan enkripsi AES dengan WPA3-SAE untuk diterapkan di dalam jaringan *wireless* 802.11ax yang dapat menghasilkan kualitas *throughput* tinggi untuk penggunaan di *channel width* 20 Mhz, 40 Mhz dan 80 Mhz. Tujuan penelitian selanjutnya adalah untuk mengetahui dampak penggunaan *beacon interval* untuk meningkatkan *throughput* ketika menerapkan *wireless security protocol* di jaringan *wireless* 802.11ax, seperti halnya penelitian yang dilakukan (Sati & Graffi, 2015) dengan tujuan mengetahui dampak dari penggunaan *beacon interval* di jaringan *wireless* standar IEEE 802.11 untuk penggunaan aplikasi dari jaringan oportunistik.

Hal ini untuk mengetahui bagaimana penggunaan *wireless security protocol* mempengaruhi kinerja jaringan *wireless* IEEE 802.11ax seperti pada

penelitian sebelumnya yang telah dilakukan oleh (Mohammed, 2016) dengan jaringan *wireless* 802.11ac dan bagaimana penggunaan *beacon interval* dapat meningkatkan *throughput* di jaringan *wireless* IEEE 802.11ax, sehingga nantinya penggunaan *wireless security protocol* lebih maksimal dan menjadi tolak ukur kinerja jaringan (Mohammed, 2016) di lingkungan *wireless* IEEE 802.11ax serta dapat meningkatkan pengetahuan terkait kinerja jaringan *wireless* IEEE 802.11ax untuk menentukan pilihan terbaik dalam memilih *wireless security protocol* yang akan diterapkan di lingkungan infrastruktur (Almatrook, 2016) jaringan IEEE 802.11ax.

Untuk penelitian yang kami lakukan dapat memberikan kontribusi ilmu pengetahuan terbaru mengenai bagaimana penggunaan *wireless security protocol* memberikan dampak terhadap kualitas *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.

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, Maraj, Efendiu, et al., 2018) serta frekuensi 5 Ghz dapat menjadi alternatif dalam penggunaan di lingkungan jaringan *wireless* untuk menunjang pekerjaan perkantoran seperti *browsing* internet, *download*, pertukaran data, dan *video conference* (Bakri et al., n.d.) sehingga nantinya didapatkan hasil kualitas *throughput* maksimal jaringan *wireless* IEEE 802.11ax. Penelitian ini juga dilakukan dengan menggunakan skenario jaringan *client server* dan jarak antara *access point* dan *client* berada

dalam jarak satu meter untuk mendapatkan kekuatan sinyal yang optimal, dan kualitas *throughput* maksimal pada jaringan *wireless* IEEE 802.11ax seperti hal nya pada penelitian yang dilakukan oleh (Kolahi & Almatrook, 2017) di dalam jaringan *wireless* IEEE 802.11ac dan penggunaan parameter *transport protocol* (TCP dan UDP) dan IP Address versi 4 (IPv4) sebagai parameter pengujian.

1.2. Rumusan Masalah

Berdasarkan permasalahan didalam penelitian yang telah dipaparkan pada latar belakang maka rumusan masalah dapat dirangkum sebagai berikut:

a. Berapa *throughput* maksimum yang dihasilkan ketika jaringan *wireless* 802.11ax tidak menerapkan *wireless security protocol* ?
b. Manakah di antara *wireless security protocol* mode WPA2 dengan enkripsi AES dan WPA3 dengan enkripsi SAE yang dapat menghasilkan kualitas *throughput* tinggi untuk penggunaan di *channel width* 20 Mhz, 40 Mhz dan 80 Mhz di jaringan *wireless* 802.11ax ?
c. Bagaimanakah efektifitas penggunaan *beacon interval* dalam meningkatkan *throughput* ketika menerapkan *wireless security protocol* untuk penggunaan di *channel width* 20 Mhz, 40 Mhz dan 80 Mhz ?

1.3. Batasan Masalah

Adapun variabel batasan yang dilakukan di dalam penelitian ini adalah sebagai berikut :

a. Perangkat Keras yang digunakan di dalam penelitian meliputi :

1) Penelitian ini menggunakan *Access Point indoor* yaitu TPlink Archer AX5400 *Dual Band* Gigabit Wi-Fi 6 sebagai pemancar jaringan *wireless*, dimana *Access Point* ini menggunakan *wireless chipset* seri *Broadcom* BCM43684KRFBG untuk *wireless* frekuensi 5 Ghz dan seri *Broadcom* BCM6750 untuk *wireless* frekuensi 2.4 Ghz.

2) Penelitian ini menggunakan *wireless Card* TP-LINK AX3000 sebagai penerima jaringan *wireless*, dimana *wireless card* ini menggunakan *chipset* Intel Wi-Fi 6 *Chipset*.

3) Penelitian ini menggunakan Server dengan spesifikasi sebagai berikut :

Tabel 2.1 Spesifikasi Perangkat Keras Server

Processor	Intel Xeon E-2224G 3.5GHz
RAM	1x 8GB DDR4 UDIMM
Harddisk	1TB 7.2K Entry SATA 3.5in
LAN *Card* 1	Intel I219-LM Gigabit Ethernet LAN 10/100/1000
LAN *Card* 2	D-LINK *Gigabit Ethernet Adapter* DGE-560T
Power Supply	300 Watt (Single)

4) Penelitian menggunakan PC *Client* dengan spesifikasi sebagai berikut :

Tabel 2.2 Spesifikasi Perangkat Keras PC *Client*

Processor	Intel Core i9-10900 2.8Ghz Up To 5.2Ghz / Setara
RAM	DDR4 32 GB (Dual Channel 16x2)
Harddisk	SSD 128 GB
Power Supply	380 Watt

b. Sistem Operasi yang digunakan di dalam penelitian meliputi :

1) Penelitian ini menggunakan Windows Server 2016 Standar untuk Server,
2) Penelitian ini menggunakan Windows 10 *Professional* version 2004 untuk PC *Client*,

c. Program Aplikasi yang digunakan di dalam penelitian meliputi :

1) Pengujian kualitas *throughput* menggunakan aplikasi *iperf version 3*,
2) Monitoring bebas interferensi terhadap *access point* lain menggunakan aplikasi *Acrylic Wi-Fi Home – WiFi Scanner*,

d. Parameter percobaan yang dilakukan dalam penelitian ini meliputi :

1) Penelitian ini hanya menguji kualitas *throughput* jaringan IEEE 802.11ax,
2) Penelitian ini hanya menggunakan frekuensi 5 Ghz, dan dilakukan di dalam ruangan (*indoor*) dengan kondisi tidak adanya interferensi dengan *access point* lain yang bekerja di frekuensi 5 Ghz,
3) Penelitian ini menggunakan pita frekuensi (*channel*) 40 (*center frequency* = 5 200 Mhz) seperti halnya pada penelitian (Mohammed 2016) dan pita frekuensi ini merupakan pita frekuensi yang bebas digunakan sesuai dengan Peraturan Menteri Komunikasi dan Informatika Republik

Indonesia Nomor 1 Tahun 2019 Pasal 7 huruf b yang mengatur penggunaan pita frekuensi radio untuk *access point indoor* dengan rentang 5 150 – 5 250 Mhz.

4) Penelitian ini menggunakan *Open Security*, WPA2 dengan enkripsi AES dan WPA3 dengan enkripsi SAE sebagai *wireless security protocols*,
5) Penelitian ini menggunakan *channel width* 20 Mhz, 40 Mhz, dan 80 Mhz,
6) Penelitian ini menggunakan pengalamatan ip address *static* dan IPv4,
7) Penelitian ini menggunakan protokol TCP dan UDP,
8) Penelitian ini menggunakan *default Advanced Setting*,
9) Penelitian ini menggunakan topologi *basic service set*, dimana jarak antara pemancar dengan penerima adalah 1 meter dan tidak terhubung ke jaringan internet.
10) Penelitian ini menggunakan variasi ukuran paket yang diuji untuk masing-masing skenario adalah 128, 384, 640, 1152 dan 1408 KBytes seperti pada penelitian yang dilakukan (Mohammed 2016) dan (Samad S. Kolahi and Almatrook 2017).
11) Penelitian ini menggunakan variasi ukuran *beacon interval* untuk masing-masing skenario adalah 50, 100, 500, 750 dan 1000 ms seperti pada penelitian yang dilakukan (Bankov et al. 2016), (Pratama et al. 2017), dan (Sati and Graffi 2015) .

1.4. Tujuan Penelitian

Terdapat tiga hal yang ingin dicapai dari penelitian ini adalah sebagai berikut :

a. Untuk mengetahui *throughput* maksimum jaringan *wireless* 802.11ax,
b. Untuk mengetahui di antara *wireless security protocol* mode WPA2 dengan enkripsi AES dan WPA3 dengan enkripsi SAE yang dapat menghasilkan kualitas *throughput* tinggi untuk penggunaan di *channel width* 20 Mhz, 40 Mhz dan 80 Mhz ?
c. Untuk mengetahui efektifitas penggunaan *beacon interval* dalam meningkatkan *thorughput* ketika menerapkan *wireless security protocol* untuk penggunaan di *channel width* 20 Mhz, 40 Mhz dan 80 Mhz ?

1.5. Manfaat Penelitian

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

a. Dapat membantu para peneliti dan pengguna dalam pemilihan *wireless security protocols* di antara WPA2 dengan enkripsi AES atau WPA3 dengan enkripsi SAE di dalam merancang dan membangun jaringan *wireless* menggunakan standarisasi IEEE 802.11ax.
b. Mendapatkan pengetahuan mengenai kualitas *throughput* dan keunggulan dari jaringan *wireless* 802.11ax.
c. Mendapatkan pengetahuan mengenai pengaruh penggunaan *beacon interval* di dalam jaringan *wireless*.

BAB II

TINJAUAN PUSTAKA

2.1. Tinjauan Pustaka

Berikut ini adalah beberapa ulasan jurnal tentang penelitian terdahulu berkenaan dengan data dan metode yang digunakan penulis sebagai acuan.

Berdasarkan penelitian sebelumnya terkait analisis kualitas *throughput* jaringan *wireless* 802.11ac berdasarkan penggunaan WEP, WPA dan WPA2 yang dilakukan oleh Talal Mohammed Alghamdi (2019), menunjukkan bahwa kualitas *throughput* data yang dihasilkan ketika jaringan *wireless* tidak menerapkan sistem keamanan hasilnya lebih tinggi dibandingkan ketika sistem keamanan diterapkan di dalam jaringan *wireless*. 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 Thanaphon Pattanasophon dkk (2017) melakukan penelitian mengenai dampak penggunaan WEP, WPA, dan WPA2 terhadap kualitas *throughput* jaringan wireless 802.11ac dengan membandingkan parameter penggunaan IPv4 dan IPv6, penelitian ini menunjukan bahwa penggunaan *wireless security protocol* WEP, WPA, dan WPA2 terhadap IPv4

dan 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 Samad S. Kolahi dkk (2017), penelitian ini bertujuan untuk mengetahui dampak penggunaan protokol keamanan WPA2 (WiFi Protected Access 2) dan *open system* (No security) terhadap kualitas *throughput* jaringan wireless 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, dengan 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 di dalam penelitian ini penulis akan melakukan penelitian berdasarkan konsep yang dilakukan oleh Thanaphon Pattanasophon dkk (2017). Perbedaan yang akan dilakukan adalah pengujian dilakukan dengan menggunakan standarisasi 802.11ax dan *wireless security protocols* yang digunakan WPA, WPA2, dan WPA3. Skenario topologi jaringan mengadopsi di dalam penelitian Talal Mohammed Alghamdi (2019) yang menggunakan skenario *client server*.

2.2. Keaslian Penelitian

Tabel 2.3. Matriks literatur review dan posisi penelitian

Analisis Dampak Penggunaan *Wireless Security Protocol* (NOS, WPA2-AES dan WPA3-SAE) Terhadap Kualitas *Throughput* Jaringan *Wireless* IEEE 802.11ax

No	Judul	Peneliti, Media, Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
1	*Throughput Analysis* of IEEE WLAN "802.11 ac" Under WEP, WPA, and WPA2 Security Protocols	Talal Mohammed Alghamdi, International Journal of Computer Networks (IJCN), Volume (9) : Issue (1) : 2019	Penelitian ini bertujuan untuk mengetahui dampak penggunaan protokol keamanan WEP (Wired Equivalent Privacy), WPA (WiFi Protected Access), dan WPA2 (WiFi Protected Access 2) terhadap kualitas *throughput* WLAN IEEE 802.11 ac.	Hasil penelitian menunjukkan bahwa kualitas *throughput* ketika jaringan wireless tidak menggunakan sistem keamanan hasilnya lebih tinggi dibandingkan dengan penggunaan sistem keamanan. Namun, hasil menunjukkan bahwa throughput memiliki hasil yang berbeda untuk sistem keamanan yang berbeda di dalam lalu lintas TCP / UDP dengan IPV4 & IPV6.	penelitian ini menggunakan IEEE 802.11ac, protokol keamanan jaringan yang digunakan WEP, WPA, dan WPA2, tidak menggunakan parameter *channel width*, menggunakan PC Desktop yang dijadikan sebagai Server, menggunakan kabel UTP Cat5e kabel transmisi, tidak di jelaskan lingkungan pengujian terbebas dari interferensi perangkat lain.	Penelitian selanjutnya menggunakan IEEE 802.11ax, , dengan WPA2 AES dan WPA3 SAE, menggunakan variasi channel width 20 Mhz, 40 Mhz dan 80 Mhz menggunakan Server sesungguhnya untuk dijadikan Server pengujian, menggunakan kabel UTP Cat6 dan lingkungan pengujian terbebas dari interferensi.

Tabel 2.3. (Lanjutan)

No	Judul	Peneliti, Media, Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
2	Impact of Security on Bandwidth and Latency in IEEE 802.11ac Client-to-Server WLAN	Samad S. Kolahi, A. A. Almatrook, Ninth International Conference on Ubiquitous and Future Networks (ICUFN), 2017	Penelitian ini bertujuan untuk mengetahui dampak penggunaan protokol keamanan WPA2 (WiFi Protected Access 2) dan open system (No security) terhadap kualitas *throughput* WLAN IEEE 802.11 ac.	Hasil dari penelitian ini menunjukkan bahwa, dengan mengimplementasikan sistem keamanan WPA2, kualitas throughput pada protokol TCP dan penggunaan IPv4 dan IPv6 mengalami penurunan sebesar 16,79% dan 10,22% sedangkan Throughput UDP menurun sebesar 18.07% dan 12,99% untuk IPv4 dan IPv6.	Di dalam penelitian ini menggunakan IEEE 802.11ac, protokol keamanan jaringan yang digunakan hanya open system dan WPA2, hanya menggunakan variasi *channel width* 80 Mhz, menggunakan PC Desktop yang dijadikan sebagai Server, masih menggunakan kabel UTP Cat5e untuk kabel transmisi,dan tidak di jelaskan lingkungan pengujian terbebas dari interferensi dengan perangkat lain.	Penelitian selanjutnya menggunakan IEEE 802.11ax, , dengan WPA2 AES dan WPA3 SAE, menggunakan variasi channel width 20 Mhz, 40 Mhz dan 80 Mhz menggunakan Server sesungguhnya untuk dijadikan Server pengujian, menggunakan kabel UTP Cat6 dan lingkungan pengujian terbebas dari interferensi.

Tabel 2.3. (Lanjutan)

No	Judul	Peneliti, Media, Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
3	A Study on Performance of IPv4, IPv6 on Wireless Network (IEEE 802.11ac) with Wireless Security Protocols (WEP, WPA and WPA2)	Thanaphon Pattanasophon,Sita Thanee,Sukrita Limpayaraya,Thongchai Kaewkiriya, TNI Journal of Engineering and Technology Vol.5 No.1, 2017	Penelitian ini bertujuan untuk membandingkan data loss rate, delay, dan throughput jaringan wireless 802.11ac dengan menggunakan parameter 6 pola yaitu menentukan percobaan IPv4 dan IPv6 menggunakan WEP, WPA dan WPA2	Hasil dari penelitian dampak penggunaan wireless security protocol WEP, WPA, dan WPA2 terhadap IPv4 dan IPv6 menunjukan bahwa IPv4 lebih stabil dibandingkan IPv6. Terutama pada kualitas throughput yang dihasilkan	Di dalam penelitian ini masih menggunakan standarisasi IEEE 802.11ac, Protokol keamanan jaringan yang digunakan hanya WEP, WPA, dan WPA2. Tidak menggunakan parameter *channel width* di dalam penelitian, dan Tidak di jelaskan pengujian terbebas dari interferensi.	Penelitian selanjutnya menggunakan standarisasi yang lebih baru yaitu IEEE 802.11ax, Protokol keamanan yang digunakan WPA2 AES dan versi terbaru yaitu WPA3 SAE, Menggunakan parameter channel width 20 Mhz, 40 Mhz dan 80 Mhz untuk mengetahui throughput yang dihasilkan dan Lingkungan pengujian terbebas dari interferensi perangkat lainnya.

Tabel 2.3. (Lanjutan)

No	Judul	Peneliti, Media, Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
4	Performance Study of the Impact of Security on 802.11ac Networks	Anthony Tsetse, Emilien Bouniord, Patrick Appiah-Kubi, Samuel Tweneboah-Kodua, Information Technology New Generations (pp.11-17) Publisher: Springer, Cham, 2018	Penelitian ini bertujuan untuk mengetahui dampak penggunaan *wireless security modes* (No Security, Personal dan Enterprise Security) terhadap kualitas throughput, delay, jitter, loss ratio and connection time.	Hasil dari penelitian bahwa peningkatan kinerja ketika tidak menerapkan sistem keamanan dibandingkan ketika menggunakan sistem keamanan. Untuk kualitas throughput, peningkatan berkisar antara 1,6 dan 8,2% tergantung penggunaan protokol (TCP / UDP) dan jaringan (IPv4 / IPv6) dan untuk delay peningkatan antara 2,8 dan 7,9% ketika tidak menggunakan sistem keamanan. Dan untuk Jitter, Loss Ratio and connection time yang dialami antara 1,3 dan 18,6%.	Peneliti : 1. Di dalam penelitian ini masih menggunakan standarisasi IEEE 802.11ac 2. Protokol keamanan jaringan yang digunakan hanya Open System, WPA2/AES dan RADIUS. 3. Tidak menggunakan parameter *channel width* di dalam penelitian, 4. Tidak di jelaskan pengujian terbebas dari interferensi perangkat lain	Penelitian selanjutnya menggunakan standarisasi yang lebih baru yaitu IEEE 802.11ax, Protokol keamanan yang digunakan WPA2 AES dan versi terbaru yaitu WPA3 SAE, Menggunakan parameter channel width 20 Mhz, 40 Mhz dan 80 Mhz untuk mengetahui throughput yang dihasilkan dan Lingkungan pengujian terbebas dari interferensi.

Tabel 2.3. (Lanjutan)

No	Judul	Peneliti, Media, Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
5	The Impact of Human Shadowing/Movement on Performance of 802.11ac Client-to-Server WLAN	Samad S. Kolahi and Abdulbasit A. Almatrook, International Journal of Computing and Digital Systems, 2019	Di dalam penelitian ini bertujuan untuk mengetahui dampak perpindahan pengguna ketika terkoneksi dengan Access Point di jaringan wireless IEEE 802.11ac dengan parameter pengujian menggunakan IPv4, IPv6, dan protokol TCP / UDP.	Hasil penelitian ini menunjukkan bahwa secara rata-rata, dari parameter TCP dan UDP kinerja jaringan wireless dengan adanya perpindahan pengguna menghasilkan throughput yang lebih rendah. Untuk IPv4, kehadiran pergerakan pengguna menurunkan throughput TCP sebesar 12.76% dan throughput UDP sebesar 9.66%. Untuk IPv6 dengan pergerakan pengguna throughput TCP dan UDP berkurang masing-masing sekitar 13,38% dan 8,74%.	Peneliti : 1. Di dalam penelitian ini masih menggunakan standarisasi IEEE 802.11ac 2. Protokol keamanan jaringan yang digunakan hanya WPA2, 3. Tidak menggunakan parameter *channel width* di dalam penelitian, 4. Penelitian ini hanya dilakukan di dalam ruangan dan tidak dijelaskan lingkungan pengujian terbebas dari interferensi.	Penelitian selanjutnya menggunakan standarisasi yang lebih baru yaitu IEEE 802.11ax, Protokol keamanan yang digunakan WPA2 AES dan versi terbaru yaitu WPA3 SAE, Menggunakan parameter channel width 20 Mhz, 40 Mhz dan 80 Mhz untuk mengetahui throughput yang dihasilkan dan Lingkungan pengujian terbebas dari interferensi..

Tabel 2.3. (Lanjutan)

No	Judul	Peneliti, Media, Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
6	Performance Comparison of Peer-Peer vs Client-Server 802.11ac WLAN using 80Mhz Channel Size	Samad S. Kolahi, Ahmad Khalid Sooran, Muhammad Mazhar Ullah Khan, and Mohammed Faroq Nasim. International Journal of Computing and Digital Systems, 2019.	Tujuan dari penelitian ini untuk mengetahui dampak penggunaan *wireless security* WPA2 terhadap kinerja jaringan wireless 802.11ac (bandwidth, Round Trip Time (RTT), dan utilisasi CPU) dengan menggunakan parameter IPv4, IPv6, TCP, UDP, peer to peer, dan client server.	Hasil penelitian ini menunjukan bahwa protokol TCP, WLAN client-server dengan IPv4 memiliki throughput tertinggi yaitu 195 Mbps untuk ukuran paket 128 Bytes dan 620 Mbps untuk ukuran paket 1408 Bytes sedangkan peer to peer dengan IPv6 memiliki throughput terendah mulai dari 79Mbps untuk 128 Paket byte dan 335 Mbps untuk paket 1408 Bytes. Untuk UDP, throughput tertinggi dicapai lagi oleh client-server dengan IPv4.	Peneliti : 1. Di dalam penelitian ini masih menggunakan standarisasi IEEE 802.11ac 2. Protokol keamanan jaringan yang digunakan hanya WPA2, 3. Hanya menggunakan *channel width* 80 Mhz di dalam penelitian,	Penelitian selanjutnya menggunakan standarisasi yang lebih baru yaitu IEEE 802.11ax, Protokol keamanan yang digunakan WPA2 AES dan versi terbaru yaitu WPA3 SAE, Menggunakan parameter channel width 20 Mhz, 40 Mhz dan 80 Mhz untuk mengetahui throughput yang dihasilkan dan Lingkungan pengujian terbebas dari interferensi.

Tabel 2.3. (Lanjutan)

No	Judul	Peneliti, Media, Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
7	Evaluation of WEP, WPA and WPA2 Security Protocols on 802.11ac Client to Server WLAN Performance	Alghamdi Talal Mohammed. A thesis submitted in partial fulfilment of the requirements for the degree of Master of Computing Unitec Institute of Technology, 2016	Tujuan dari penelitian ini adalah untuk mengetahui dampak dari penggunaan protokol keamanan ketika diaktifkan dan dinonaktifkan terhadap kinerja jaringan WLAN 802.11ac Selain itu, penelitian ini juga menggunakan IPv4 dan IPv6, dengan jenis paket TCP / UDP.	Hasil penelitian menunjukkan di antara 3 protokol keamanan yang diuji; WEP, WPA, WPA2. Protokol WPA memiliki hasil terbaik untuk performa jaringan kecuali *throughput* data. Berdasarkan hasil tersebut dapat disimpulkan bahwa WPA dengan protokol UDP di bawah IPv6 adalah konfigurasi terbaik untuk memiliki ekstensi kinerja terbaik 802.11ac di bawah protokol keamanan diaktifkan.	Peneliti : 1. Di dalam penelitian ini masih menggunakan standarisasi IEEE 802.11ac 2. Protokol keamanan jaringan yang digunakan WEP, WPA, WPA2, 3. Hanya menggunakan *channel width* 40 Mhz di dalam penelitian,	Penelitian selanjutnya menggunakan standarisasi yang lebih baru yaitu IEEE 802.11ax, Protokol keamanan yang digunakan WPA2 AES dan versi terbaru yaitu WPA3 SAE, Menggunakan parameter channel width 20 Mhz, 40 Mhz dan 80 Mhz untuk mengetahui throughput yang dihasilkan dan Lingkungan pengujian terbebas dari interferensi.

Tabel 2.3. (Lanjutan)

No	Judul	Peneliti, Media, Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
8	Analisis Performa IEEE 802.11n dan IEEE 802.11ac	Erwin Gunawan, Jurnal Teknik Vol. 13 No. 1 Maret 2020	Tujuan penelitian untuk mengkomparasi kedua standar pada jaringan internal yang berfungsi secara penuh di lingkungan dalam ruang (indoor) universitas. Parameter delay, packet loss, serta throughput dari kedua standar pada saat dilewatkan trafik video, diukur dalam penelitian ini.	Hasil penelitian menunjukan bahwa pada jarak 5m (LoS) dari AP, IEEE 802.11n dengan channel width 40 MHz menghasilkan rata-tara penguatan bandwidth sebesar 54% dibanding dengan channel width 20 MHz. Pada kondisi yang sama IEEE 802.11ac dengan channel width 40 MHz menghasikan penguatan 64% dibanding dengan 20 MHz.	Peneliti : 1. Di dalam penelitian ini masih menggunakan standarisasi IEEE 802.11ac 2. Tidak menggunakan Protokol keamanan jaringan 3. Hanya menggunakan *channel width* 40 Mhz di dalam penelitian.	Penelitian selanjutnya menggunakan standarisasi yang lebih baru yaitu IEEE 802.11ax, Protokol keamanan yang digunakan WPA2 AES dan versi terbaru yaitu WPA3 SAE, Menggunakan parameter channel width 20 Mhz, 40 Mhz dan 80 Mhz untuk mengetahui throughput yang dihasilkan dan Lingkungan pengujian terbebas dari interferensi.

Tabel 2.3. (Lanjutan)

No	Judul	Peneliti, Media, Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
9	Handover Analysis Of Data Services In Wireless Distribution System (WDS) Using IEEE 802.11AC Standards In Telecommunicati on Laboratory Polines	Arya Pitaka, Muhammad Anif., Agus Rochadi , JAICT, Journal of Applied Information and Communication Technologies, Vol.2, No.2, 2017	Penelitian ini dilakukan untuk mengetahui tentang pengaruh proses handover terhadap kualitas layanan data dengan parameter Quality of Service (QoS) yaitu throughput, delay, jitter dan packet loss di dalam jaringan WLAN 802.11ac	Hasil penelitian ini menunjukan bahwa nilai throughput rata-rata pada layanan download sebesar 12,94 Mbps, layanan upload sebesar 11,22 Mbps dan layanan video streaming sebesar 3,66 Mbps. Nilai rata-rata delay pada layanan download sebesar 0,99 ms, layanan unggah 1,19 ms dan layanan video streaming 3,07 ms. Nilai rata-rata jitter pada layanan unduh 0,36 ms, pada layanan unggah 0,35 ms dan layanan video streaming 3,66 ms. Nilai rata-rata packet loss pada layanan download sebesar 2,57%, layanan upload 5,00% dan layanan video streaming 7,05%.	Peneliti : 1. Di dalam penelitian ini masih menggunakan standarisasi IEEE 802.11ac 2. Tidak menggunakan Protokol keamanan jaringan 3. Hanya menggunakan *channel width* 40 Mhz di dalam penelitian,	Penelitian selanjutnya menggunakan standarisasi yang lebih baru yaitu IEEE 802.11ax, Protokol keamanan yang digunakan WPA2 AES dan versi terbaru yaitu WPA3 SAE, Menggunakan parameter channel width 20 Mhz, 40 Mhz dan 80 Mhz untuk mengetahui throughput yang dihasilkan dan Lingkungan pengujian terbebas dari interferensi.

Tabel 2.3. (Lanjutan)

No	Judul	Peneliti, Media, Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
10	Analisis Pengaruh Bandwidth Kanal Terhadap Konsumsi Energi Wifi 802.11ac Yang Menggunakan Sistem Keamanan Wpa Dan Wpa2 Pada Smartphone	Raziv Ravsanzhani, Electronic Theses and Dissertations (ETD) Universitas Syiah Kuala, 2016	Tujuannya untuk mengetahui pengaruh bandwidth kanal terhadap konsumsi daya dan energy pada smartphone yang terhubung ke jaringan Wifi 802.11ac, khususnya pada yang menggunakan sistem keamanan WPA dan WPA2 dan yang tidak menggunakan sistem keamanan sama sekali	Hasil penelitian ini menunjukan bahwa konsumsi daya dan energy yang paling tinggi pada pengujian tanpa sistem keamanan adalah 24,160 W dan 86,976 kJ. Pada keadaan dengan sistem keamanan WPA-TKIP konsumsi daya dan energy tertingginya adalah 0,9155 W dan 2,295 kJ, sedangkan dengan keamanan WPA2-AES konsumsi daya dan energy tertingginya adalah 26,855 W dan 96,678 kJ.	Peneliti : 1. Di dalam penelitian ini masih menggunakan standarisasi IEEE 802.11ac 2. Tidak menggunakan Protokol keamanan jaringan 3. Hanya menggunakan *channel width* 40 Mhz di dalam penelitian.	Penelitian selanjutnya menggunakan standarisasi yang lebih baru yaitu IEEE 802.11ax, Protokol keamanan yang digunakan WPA2 AES dan versi terbaru yaitu WPA3 SAE, Menggunakan parameter channel width 20 Mhz, 40 Mhz dan 80 Mhz untuk mengetahui throughput yang dihasilkan dan Lingkungan pengujian terbebas dari interferensi.

Tabel 2.3. (Lanjutan)

No	Judul	Peneliti, Media, Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
11	Implementasi Dan Analisis Access Point 5 Ghz Menggunakan Metode Manual Random Sampling Dan Converage Visualization	Maulid, Muh.Yaman, L.M. Fid Aksara, La Surimi, semanTIK, Vol.6, No.1, Jan-Jun 2020, pp. 107-114	Tujuan penelitian ini adalah untuk mengetahui kekuatan sinyal dan optimalisasi jarak terhadap penggunaan jaringan frekuensi 5 GHz.	Berdasarkan penelitian yang telah dilakukan selama implementasi dan analisis sistem hasil yang didapatkan adalah penempatan Access Point dengan kondisi tanpa hambatan mendapatkan nilai RSSI yang lebih baik dibandingkan dengan penempatan Access Point yang mempunyai hambatan. Hal ini dikarenakan yang mempengaruhi kondisi tanpa hambatan hanya terdapat pada parameter jarak sedangkan pada kondisi adanya hambatan yang mempengaruhi adalah jarak dan hambatan (bangunan-bangunan, bukit, medan dan pepohonan). Semakin jauhnya jarak yang dilalui oleh jaringan internet maka semakin banyak pula hambatan yang akan ditemukan.	Peneliti : 1. Di dalam penelitian ini masih menggunakan standarisasi IEEE 802.11ac 2. Tidak menggunakan Protokol keamanan jaringan 3. Hanya menggunakan *channel width* 40 Mhz di dalam penelitian.	Penelitian selanjutnya menggunakan standarisasi yang lebih baru yaitu IEEE 802.11ax, Protokol keamanan yang digunakan WPA2 AES dan versi terbaru yaitu WPA3 SAE, Menggunakan parameter channel width 20 Mhz, 40 Mhz dan 80 Mhz untuk mengetahui throughput yang dihasilkan dan Lingkungan pengujian terbebas dari interferensi.

Tabel 2.3. (Lanjutan)

No	Judul	Peneliti, Media, Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
12	Analisis Throughput Jaringan Lan Ad Hoc Pada Ruang Indoor Menggunakan Standar Tipbon	Achmad Guntara, Hanafi, Muhammad. JURNAL LITEK : Jurnal Listrik Telekomunikasi Elektronika, Vol.16, No.1, Maret 2019, pp. 13~18	Tujuan penelitian ini adalah untuk mengetahui kualitas throughput jaringan AD HOC	Hasil dari pengujian throughput diperoleh bahwa throughput rata-rata dari setiap file baik yang transfer data user 1 lebih cepat melakukan transfer file daripada user 2, user 3, dan user 4. Jumlah user maksimal yang dapat tersambung dalam jaringan ad hoc ini adalah 4 user. Ini disebabkan kapasitas dari bandwidth jaringan ad hoc terbatas. Selanjutnya pada proses transfer data menggunakan 3 user dan 4 user, jarak maksimalnya yaitu 5 m, dan saat jarak 10 m terjadi error.	Peneliti : 1. Di dalam penelitian ini masih menggunakan standarisasi IEEE 802.11ac 2. Tidak menggunakan Protokol keamanan jaringan 3. Hanya menggunakan *channel width* 40 Mhz di dalam penelitian.	Penelitian selanjutnya menggunakan standarisasi yang lebih baru yaitu IEEE 802.11ax, Protokol keamanan yang digunakan WPA2 AES dan versi terbaru yaitu WPA3 SAE, Menggunakan parameter channel width 20 Mhz, 40 Mhz dan 80 Mhz untuk mengetahui throughput yang dihasilkan dan Lingkungan pengujian terbebas dari interferensi.

2.3. Landasan Teori

Terdapat beberapa landasan teori yang dibutuhkan dalam penelitian ini, mulai dari landasan teori mengenai standarisasi 802.11ax, *Channel Width*, *Throughput*, *Wireless Security Protocols* (WPA, WPA2, dan WPA3), Internet Model (Protokol TCP/IP) dan *Transport Protocol* (TCP/UDP).

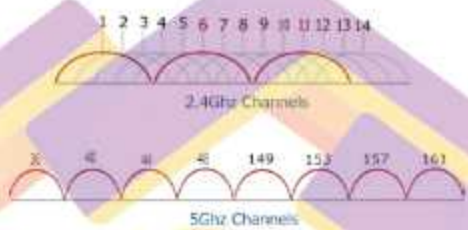
2.3.1 Standarisasi 802.11ax

WiFi 6 atau standarisasi 802.11ax adalah teknologi jaringan *wireless* terbaru yang memberikan peningkatan signifikan pada standar jaringan *wireless*. 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 *dual band* 2.4 Ghz dan 5 Ghz, mendukung hingga delapan transmisi MU-MIMO sekaligus (zhao 2019) 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 *wireless* (hidayat 2013).

2.3.2 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. (sofana 2008). 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.



Sumber : https://wifiadviser.com/archives/376

Gambar 2.1. WIFI *Channel bandwidth*

2.3.3 Throughput

Throughput merupakan perhitungan kecepatan (rate) transfer data efektif antara pengirim dan penerima, satuan yang digunakan dalam pengukuran adalah bps (*bit per second*). *Throughput* merupakan jumlah total kedatangan paket yang sukses yang diamati pada *destination* selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut (jonathan 2011).

$$Throughput = \frac{\text{jumlah data yang diterima}}{\text{waktu pengiriman data}}$$

Ada beberapa alat bantu perangkat lunak yang bisa digunakan untuk mengukur kualitas *throughput* salah satunya adalah aplikasi *iperf*, aplikasi ini menghasilkan lalu lintas dan mengukur parameter paket yang ditransmisikan

untuk TCP dan UDP (blum 2003). Dibandingkan dengan aplikasi *bandwidth generator* lainnya *iperf* memiliki hasil pengukuran *bandwidth* yang lebih tinggi (kolahi. 2011). Selanjutnya setelah dilakukan pengukuran menggunakan aplikasi *iperf* tahapan berikutnya adalah membandingkan dengan standar penilaian *throughput* menurut standar ETSI - *Telecommunication and internet protocol harmonization over network* (TIPHON). Kriteria kualitas *throughput* tersebut adalah sebagai berikut :

Tabel 2.4. Penilaian *QOS* Parameter *Throughput*

Kategori *Throughput*	*Throughput* %	Indeks
Sangat Bagus	100 %	4
Bagus	75 %	3
Sedang	50 %	2
Jelek	< 25 %	1

Sumber : TIPHON

2.3.4 *Wireless Security Protocols*

Protokol keamanan jaringan *wireless* telah melalui banyak perubahan dan peningkatan sejak tahun 1990-an untuk menjadi lebih aman dan efektif. Berbagai jenis protokol keamanan jaringan *wireless* dikembangkan untuk perlindungan jaringan *wireless* yang terpasang baik untuk pengguna di rumah hingga bisnis skala besar (mulyanta 2005). Berikut *wireless security protocol* yang banyak digunakan saat ini :

a. WPA2 (WI-FI PROTECTED ACCESS VERSI 2)

WPA2 atau WPA versi 2 merupakan pengembangan dari WPA di dalam teknologi keamanan di jaringan wireless, dimana WPA2 memiliki

perbedaan dalam hal integritas data yaitu menggunakan CBC-MAC (*Cipher Block Chaining-Message Authentication Code*) dan metode enkripsi terbaru yaitu *Advanced Encryption Standard* (AES) (surantha. 2016).

b. WPA3 (WI-FI PROTECTED ACCESS VERSI 3)

Berikutnya adalah WPA3 atau WPA versi 3 merupakan versi pembaruan dari teknologi keamanan wireless WPA2. WPA3 dikenalkan ke publik pada 25 Juni 2018, dimana pada WPA3 menggunakan metode enkripsi *Simultaneous Authentication of Equals* (SAE) yang menggantikan metode otentikasi *Pre shared key* (geier 2018) dengan enkripsi ini pengguna jaringan *wireless* akan terlindungi dari upaya *brute force* yang dilakukan oleh *attacker*, selain pembaruan metode enkripsi WPA3 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* (piotrowski 2019).

2.3.5 Internet Model (Protokol TCP/IP)

TCP/IP merupakan sekumpulan protokol yang terdapat di dalam jaringan komputer yang digunakan untuk berkomunikasi atau bertukar data antar komputer (syafrizal 2020), dimana protokol ini menawarkan aturan komunikasi antara satu perangkat dengan perangkat lainnya ketika proses pertukaran data berlangsung.

Model TCP / IP adalah versi singkat dari model OSI dimana model ini berisi empat lapisan, tidak seperti tujuh lapisan dalam model OSI. Lapisan tersebut adalah *Application Layer (Process), Transport Layer (Host-to-Host), Internet Layer, Network Access* (chauhan 2020).

2.3.6 *Transport Layer* (TCP dan UDP)

Di dalam model TCP/IP *transport layer* memiliki peran untuk menjaga proses komunikasi *end-to-end* (jain.2020), dimana protokol ini akan mengirimkan paket data, sekaligus akan memastikan bahwa paket diterima dengan sukses (*acknowledgement*), dan mentransmisikan ulang terhadap paket-paket yang hilang atau rusak di tengah jalan (ghayyurabbas 2019).

Terdapat dua protokol di dalam *transport layer* yaitu *Transmission Control Protocol* (TCP) yang berorientasi pada koneksi dimana pada protokol ini menggunakan proses *handshaking* (SYN, SYN-ACK dan ACK) di dalam proses komunikasi *end-to-end* nya sehingga data yang diterima dengan protokol TCP lebih terjamin karena memiliki nomor urut dan akan dipulihkan apabila terjadi kesalahan. Protokol yang kedua adalah *User Datagram Protocol* (UDP), berbeda halnya dengan TCP, protokol UDP tidak memerlukan proses *handshaking* ketika melakukan koneksi dan tidak membutuhkan tanda pengenal atau nomor urut. UDP mengirimkan data dalam aliran dan hanya memeriksa jumlah untuk memastikan bahwa data diterima tanpa kerusakan. UDP hampir tidak mengoreksi kesalahan pengiriman dan tidak peduli apabila paket hilang (klaus 2020).

2.3.5 *Beacon Interval*

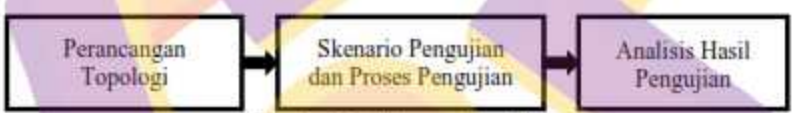
Beacon interval adalah jarak waktu pengiriman dari *beacon frames*. Perangkat AP mengirimkan dengan jarak waktu yang regular untuk menentukan posisi *user*. Pengaturan otomatis pada perangkat yang digunakan adalah 100 milliseconds (ms) atau 1 detik. Pengaturan ini dapat berbeda tergantung perangkat *Access Point* yang digunakan (Pratama et al. 2017).

BAB III

METODE PENELITIAN

3.1. Jenis, Sifat, dan Pendekatan 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 3 tahapan penelitian seperti yang terlihat di dalam gambar 3.1



Gambar 3.1. Tahapan Penelitian

3.1.1. 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 version 2004 dan terpasang *wireless card* TPLink AX3000 yang nantinya terhubung ke jaringan *wireless* menggunakan *access point indoor* TPLink Archer AX5400, 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, Maraj, and Berzati 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, Farhan, and Sujatmiko n.d.), sehingga nantinya didapatkan hasil kualitas throughput 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

Gambar 3.2. 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 192.168.1.2/24, dan untuk PC *client* menggunakan IP Address 192.168.1.3/24 serta *access Point* TPLink AX5400 yang berfungsi sebagai penghubung antara PC server dan PC *client* menggunakan IP Address 192.168.1.1/24. Selanjutnya, berbagai parameter pengujian diterapkan. Parameter yang digunakan untuk pengujian dirangkum dalam tabel 3.1.

Tabel 3.1. Parameter Untuk Pengujian

Level	Parameter
Network	*Client Server*
IP Version	IPv4
Wireless Security Protocol	*Open Security*, WPA-AES, WPA3-SAE
Packet Types	TCP, UDP
Packet Sizes	128, 384,640,1152,1408 (KBytes)
Beacon Interval	40,100,200,500,1000 (Milisecond)

Tabel 3.2. Alat Ukur Untuk Evaluasi Pengujian

Metrics	Alat Ukur
Throughput	Iperf versi 3

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

Tabel 3.3. Perangkat Keras Untuk Pengujian

Perangkat Keras	Fungsi	Spesifikasi
TP-Link Archer AX73 (AX5400)	*Wireless Access Point*	support Dual Band (2.4 GHz and 5 GHz), Support Gigabit LAN Ports and Static Link Aggregation (LAG) available with 2× LAN ports, Support WPA3 SAE.
TP-LinkAX3000 WiFi Card	*Wireless Card Adapter*	WiFi 6 PCIe Card, Up to 2400Mbps, 802.11AX Dual Band Wireless.

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 seperti pada penelitian yang dilakukan oleh (Tsetse et al. 2018) dan (Lepaja et al. 2018) karena penggunaan *iperf* sebagai aplikasi *traffic generator* memberikan hasil yang lebih tinggi dibandingkan dengan aplikasi *traffic generator* lainnya (Samad S. Kolahi et al. 2011). Dimana perintah untuk menjalankan aplikasi *iperf* menggunakan *command prompt* Microsoft Windows, berikut perintah konfigurasi yang digunakan :

Gambar 3.3. Perintah *iperf* Pada PC server yang bertindak sebagai *receiver*

Dan berikut merupakan penjelasan perintah di dalam gambar 3.3 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 *client* akan menggunakan **port 5201** ketika pengujian protokol TCP dan UDP, yang mana port 5201 adalah port *default iperf* versi 3.

Gambar 3.4. Perintah *iperf* Pada PC *client* yang bertindak sebagai transmitter untuk pengujian protokol TCP

Selanjutnya untuk penjelasan perintah di dalam gambar 3.4. yang digunakan pada PC *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 192.168.1.2 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 128 KB. 384 KB, 640 KB, 1152KB dan 1408 KB.

Gambar 3.5. Perintah *iperf* Pada PC *client* yang bertindak sebagai transmitter untuk pengujian protokol UDP

Kemudian perintah yang digunakan untuk pengujian UDP seperti ditunjukan di gambar 3.5, 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 address 192.168.1.2 adalah alamat IP address PC 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, dan perintah **–w** merupakan perintah yang digunakan untuk mengatur ukuran paket yang akan dikirimkan dan diikuti dengan menuliskan ukuran paket yang akan dikirimkan yaitu 128 KB. 384 KB, 640 KB, 1152KB dan 1408 KB.

3.1.2. Tahapan dan Skenario Pengujian

Penggunaan tahapan dan skenario pengujian di dalam penelitian ini bertujuan untuk mendapatkan nilai *throughput* tertinggi dari penggunaan mode *open security*, WPA2-AES dan WPA3-SAE ketika digunakan di *channel width* 20 Mhz, 40 Mhz dan 80 Mhz. Tujuan selanjutnya untuk mendapatkan nilai *beacon interval* terbaik yang dapat menghasilkan *throughput* tertinggi saat menerapkan *wireless security protocol* WPA2-AES dan WPA3-SAE. Dan berikut merupakan tabel skenario yang akan dilakukan :

Tabel 3.4. Skenario Pengujian

Tahap Pengujian	Skenario	Parameter Pengujian			
		Channel Width	*Protocol*	*Wireless Security*	*Beacon Interval*
1	1	20 Mhz	TCP, UDP	Open Security, WPA2-AES, WPA3-SAE	-
	2	40 Mhz	TCP, UDP	Open Security, WPA2-AES, WPA3-SAE	-
	3	80 Mhz	TCP, UDP	Open Security, WPA2-AES, WPA3-SAE	-
2	1	20 Mhz	TCP, UDP	Open Security, WPA2-AES, WPA3-SAE	✓
	2	40 Mhz	TCP, UDP	Open Security, WPA2-AES, WPA3-SAE	✓
	3	80 Mhz	TCP, UDP	Open Security, WPA2-AES, WPA3-SAE	✓

Berikut penjabaran konseptual skenario dari tabel 3.4 tersaji di bawah ini :

1. Tahap pengujian pertama adalah untuk mengetahui dampak penggunaan *wireless security protocol* terhadap *throughput* yang didapatkan oleh PC *Client*. Dimana di dalam tahap pengujian pertama ini terdiri dari tiga skenario pengujian, yaitu pada skenario pertama menggunakan *channel width* 20 Mhz, skenario kedua menggunakan *channel width* 40 Mhz dan skenario ketiga menggunakan *channel width* 80 Mhz. Setiap skenario akan menggunakan parameter uji sebagai berikut :

Tabel 3.5. Parameter Uji Tahap Pertama

Jenis	Parameter Uji
Topologi Jaringan	*Client Server*
Versi IP Address	IPv4
Mode *Wireless Security*	*Open Security*, WPA-AES dan WPA3-SAE
Tipe Paket	TCP, UDP
Ukuran Paket	128 KB, 384 KB, 640 KB, 1152 KB, 1408 KB

Seperti halnya pada penelitian (Samad S. Kolahi and Almatrook 2019) tahapan pada setiap skenario pengujian dilakukan dengan protokol TCP dan UDP secara bergantian sebagai parameter tipe paket yang diujikan. Dimana pengujian terlebih dahulu menggunakan *wireless security protocol* mode *open security*, kemudian dilakukan pengukuran *throughput* menggunakan aplikasi *iperf* versi 3 dengan variasi paket data yang dikirimkan dari PC *client* ke *server* adalah 128 KB, 384 KB, 640 KB, 1152 KB dan 1408 KB. 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 ditunjukan pada tabel 3.7. Pengujian kemudian dilanjutkan dengan mengganti mode *wireless security protocol* menjadi WPA2-AES dan WPA3-SAE.

2. Tahap pengujian kedua adalah untuk mengetahui dampak penggunaan *beacon interval* untuk meningkatkan *throughput* ketika menerapkan *wireless security protocol*. Dimana di dalam tahap pengujian pertama ini terdiri dari tiga skenario pengujian, dimana pada skenario pertama menggunakan *channel width* 20 Mhz, skenario kedua menggunakan *channel width* 40 Mhz dan

skenario ketiga menggunakan *channel width* 80 Mhz. Berikut parameter uji dan skenario yang digunakan :

Tabel 3.6. Parameter Uji Tahap Kedua

Jenis	Parameter Uji
Topologi Jaringan	*Client Server*
Versi IP Address	IPv4
Mode *Wireless Security*	*Open Security*, WPA-AES dan WPA3-SAE
Tipe Paket	TCP, UDP
Ukuran Paket	128 KB, 384 KB, 640 KB, 1152 KB, 1408 KB
Ukuran nilai *Beacon*	50 ms, 100 ms, 500 ms, 750 ms, 1000 ms

Seperti halnya pada pengujian pertama, pada pengujian kedua tahapan setiap skenario juga dilakukan dengan menggunakan protokol TCP dan UDP secara bergantian. Namun yang membedakan adalah pada pengujian kedua ini dengan menambahkan parameter uji *beacon interval* untuk mengetahui peningkatan *throughput* yang didapatkan seperti halnya pada penelitian (Sati and Graffi 2015). Selanjutnya langkah pertama pada setiap skenario terlebih dahulu menggunakan *wireless security protocol* mode *open security*, kemudian nilai *beacon interval* dirubah menjadi 50 ms selanjutnya dilakukan pengukuran *throughput* menggunakan aplikasi *iperf* versi 3 dengan variasi paket data yang dikirimkan dari PC *client* ke *server* adalah 128 KB, 384 KB, 640 KB, 1152 KB dan 1408 KB. 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 ditunjukan pada tabel 3.7. Pengujian kemudian dilanjutkan dengan mengganti

mode *wireless security protocol* menjadi WPA2-AES dan WPA3-SAE dan merubah nilai *beacon interval* menjadi 500 ms, 750 ms dan 1000 ms untuk setiap mode *wireless security protocol* yang digunakan.

Tabel 3.7. Tabel Hasil Pengujian

Channel Width 20 Mhz / 40 Mhz / 80 Mhz

No	Mode Security	Packet Size	100ms (Default)	50 ms	500 ms	750 ms	1000 ms
1	Open Security/ WPA2-AES/ WPA3-SAE	128 KB					
		384 KB					
		640 KB					
		1152 KB					
		1408 KB					

3.1.3. Analisis Hasil Pengujian

Setelah data-data yang diperlukan terkumpul, untuk langkah selanjutnya adalah melakukan analisis untuk mengolah data tersebut menjadi sebuah informasi. Analisis hasil akan menyajikan perbandingan pada penggunaan protokol TCP dan UDP. Tahap analisis terdiri dari dua tahapan yaitu pada tahap pertama analisa yang dilakukan adalah berdasarkan data pengujian dampak penggunaan *wireless security protocol* dengan mode *open security*, WPA2-AES dan WPA3-SAE saat digunakan di *channel width* 20 Mhz, 40 Mhz dan 80 Mhz. Selanjutnya pada tahap kedua analisa yang dilakukan adalah berdasarkan pengujian dampak penggunaan *beacon interval* untuk meningkatkan *throughput* ketika menggunakan *wireless security protocol* mode WPA2-AES dan WPA3-SAE saat digunakan di *channel width* 20 Mhz, 40 Mhz dan 80 Mhz.

3.2 Metode Pegumpulan Data

Pada tahap pengumpulan data penulis mengumpulkan berbagai data dari beberapa sumber yaitu sebagai berikut:

3.2.1. Metode Studi Literatur

Penulis melakukan pencarian data melalui internet untuk mendapatkan informasi yang berkaitan dengan IEEE 802.11ax, *wireless security protocols*, *channel width*, dan *beacon interval*. Jenis data yang dihasilkan berupa data dari perkembangan standarisasi jaringan *wireless* dan pengaruh penggunaan *wireless security protocol* dan beacon interval di dalam jaringan *wireless*.

3.2.2. Metode Kepustakaan

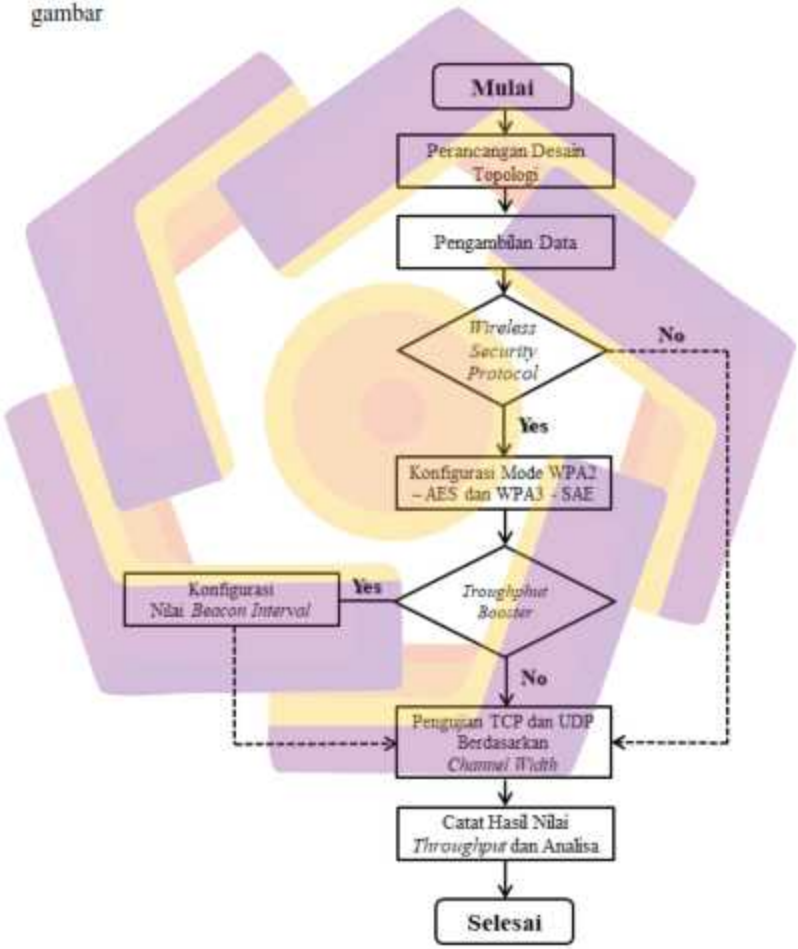
Penulis melakukan pengumpulan data dengan mengkaji teori melalui buku-buku yang relevan dan sumber lainnya dari internet. Jenis data yang didapatkan berupa teori-teori tentang IEEE 802.11ax, *wireless security protocols*, *channel width*, dan *beacon interval*.

3.2.3. Metode Observasi

Penulis melakukan observasi dengan melakukan percobaan berdasarkan skenario topologi yang sudah ditentukan sebelumnya, langkah-langkah percobaan dimulai dari konfigurasi sistem dan perangkat sampai dengan pengujian dan pengukuran dari alat ukur yang digunakan untuk mengukur parameter-parameter yang telah ditentukan.

3.3 Alur Penelitian

Terdapat beberapa tahapan dalam melakukan proses penelitian dampak penggunaan *wireless security protocol* terhadap kualitas *throughput* jaringan wireless 802.11ax. Tahapan-tahapan tesebut secara garis besar dapat dilihat pada gambar



Gambar 3.6. Alur Penelitian

Gambar 3.6 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 Tahap Pertama (*Wireless Security Protocols*) :

   Di dalam tahap pengujian pertama ini terdiri dari tiga skenario pengujian untuk protokol TCP dan UDP, yaitu pada skenario pertama menggunakan *channel width* 20 Mhz, skenario kedua menggunakan *channel width* 40 Mhz dan skenario ketiga menggunakan *channel width* 80 Mhz. Dimana pada setiap skenario paramater yang akan diuji seperti *wireless security protocol Open Security*, WPA2-AES dan WPA3-SAE serta ukuran paket yang akan digunakan adalah 128 KB, 384 KB, 640 KB, 1152 KB dan 1408 KB.

c. Pengambilan Data Tahap Kedua (*Throughput Booster*):

   Seperti halnya pada tahap pertama pada pengambilan data di dalam tahap kedua ini terdiri dari tiga skenario, penggunaan parameter uji *wireless security protocols* WPA2-AES dan WPA3-SAE, ukuran paket yang akan digunakan adalah 128 KB, 384 KB, 640 KB, 1152 KB dan 1408 KB serta merubah nilai *beacon interval* menjadi 500 ms, 750 ms dan 1000 ms untuk setiap mode *wireless security protocol* yang digunakan.

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.

BAB IV

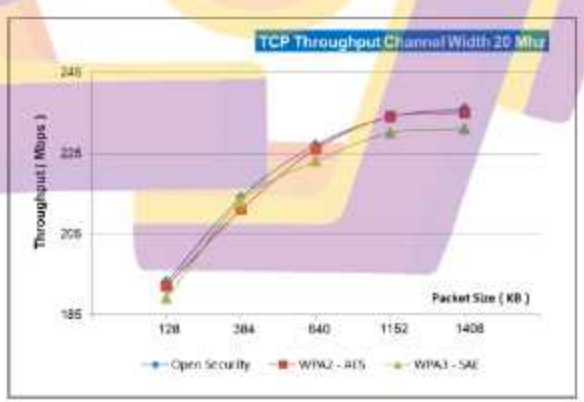
HASIL PENELITIAN DAN PEMBAHASAN

Pada pengujian ini terdiri dari 2 tahap yang dilakukan, tahap pertama adalah untuk mengetahui pengaruh penggunaan *wireless security protocol* terhadap kualitas *throughput* yang dihasilkan, selanjutnya pada tahap kedua adalah untuk mengetahui pengaruh penggunaan *beacon interval* dalam meningkatkan kualitas throughput yang dihasilkan ketika menerapkan *wireless security protocol* baik mode *open secur*ity, WPA2 – AES maupun WPA3 – SAE. di dalam *channel width* 20 Mhz, 40 Mhz dan 80 Mhz. Berikut adalah hasil dan pembahasan dari pengujian yang telah dilakukan :

4.1 Hasil Pengujian Perbandingan Penggunaan *Wireless Security Protocol*

4.1.1 Perbandingan Untuk *Channel Width* 20 Mhz

a. Hasil Pengujian TCP

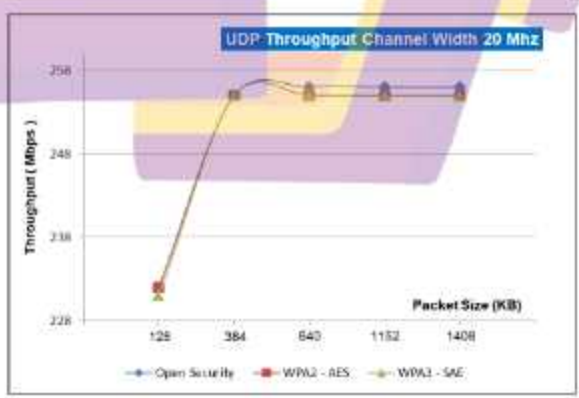


Gambar 4.1 Hasil Pengujian TCP *Throughput Channel Width* 20 Mhz

Throughput di dalam komunikasi jaringan merupakan jumlah *byte* yang dapat dikirimkan dari pengirim untuk penerima. Beberapa faktor yang dapat mempengaruhi kualitas *throughput* di antaranya penggunaan protokol jaringan seperti TCP dan UDP, protokol keamanan, ukuran paket yang dikirimkan.

Berdasarkan hasil pengujian di atas menunjukan bahwa ukuran paket yang dikirimkan akan meningkatkan *throughput* yang dihasilkan dan pada penggunaan *wireless security protocol* baik WPA2 – AES maupun WPA3 – SAE mengalami penurunan bila dibandingkan ketika jaringan *wireless* tidak menerapkan *wireless security protocol* (*Open Security*). Namun pada penggunaan WPA2 – AES lebih baik bila dibandingkan dengan WPA3 – SAE dimana hal ini ditunjukan dengan penurunan *throughput* hanya 1 Mbps (0,5%) ditunjukan ketika pengiriman paket sebesar 128 KB, 640 KB dan 1408 KB sedangkan untuk penggunaan WPA3 – SAE mengalami penurunan terbesar hingga 5 Mbps (2,1%) ditunjukan ketika pengiriman paket sebesar 1408 KB.

b. Hasil Pengujian UDP

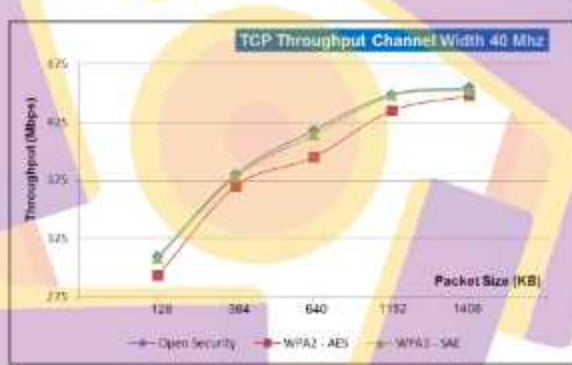


Gambar 4.2 Hasil Pengujian TCP *Throughput Channel Width* 20 Mhz

Pada pengujian untuk protokol UDP seperti ditunjukan grafik di atas menunjukan bahwa penggunaan *wireless security protocol* baik WPA2 – AES maupun WPA3 – SAE mengalami penurunan bila dibandingkan ketika jaringan *wireless* tidak menerapkan *wireless security protocol* (*Open Security*) seperti halnya pada pengujian protokol TCP. Baik pada penggunaan WPA2 – AES dan WPA3 – SAE mengalami penurunan sebesar 1 Mbps (0,5%) hal ini ditunjukan ketika pengiriman paket 640 KB, 1152 KB dan 1408 KB.

4.1.2 Perbandingan Untuk *Channel Width* 40 Mhz

a. Hasil Pengujian TCP



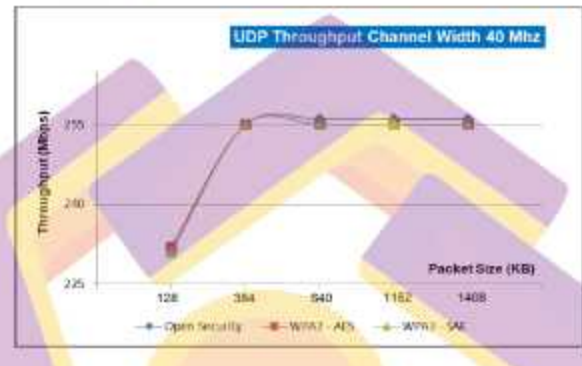
Gambar 4.3 Hasil Pengujian TCP *Throughput Channel Width* 40 Mhz

Pada penggunaan *channel width* 40 Mhz, hasil pengujian protokol TCP menunjukan bahwa penggunaan *wireless security protocol* baik WPA2 – AES maupun WPA3 – SAE mengalami penurunan bila dibandingkan ketika jaringan *wireless* tidak menerapkan *wireless security protocol* (*Open Security*).

Namun pada penggunaan WPA3 – SAE lebih baik bila dibandingkan dengan WPA2 – AES dimana hal ini ditunjukan dengan penurunan *throughput*

terbesar hanya 4 Mbps (0,9%) ditunjukan ketika pengiriman paket sebesar 640 KB sedangkan untuk penggunaan WPA2 – AES mengalami penurunan hingga 23 Mbps (5,5%) ditunjukan ketika pengiriman paket sebesar 640 KB.

b. Hasil Pengujian UDP



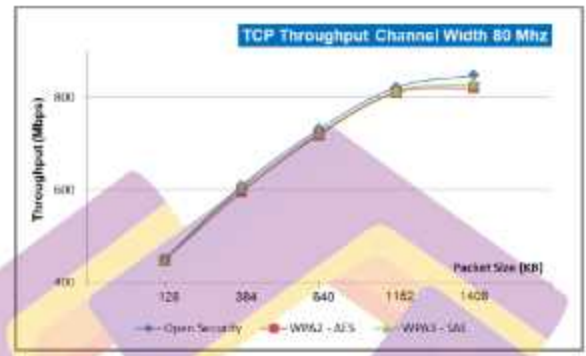
Gambar 4.4 Hasil Pengujian UDP *Throughput Channel Width* 40 Mhz

Pada penggunaan *channel width* 40 Mhz, hasil pengujian protokol UDP menunjukan bahwa penggunaan *wireless security protocol* baik WPA2 – AES maupun WPA3 – SAE mengalami penurunan bila dibandingkan ketika jaringan *wireless* tidak menerapkan *wireless security protocol* (*Open Security*).

Baik pada penggunaan WPA2 – AES maupun WPA3 – SAE mengalami penurunan *throughput* sebesar 1 Mbps (0,5%) ditunjukan ketika pengiriman paket sebesar 640 KB, 1152 KB dan 1408 KB.

4.1.3 Perbandingan Untuk *Channel Width* 80 Mhz

a. Hasil Pengujian TCP

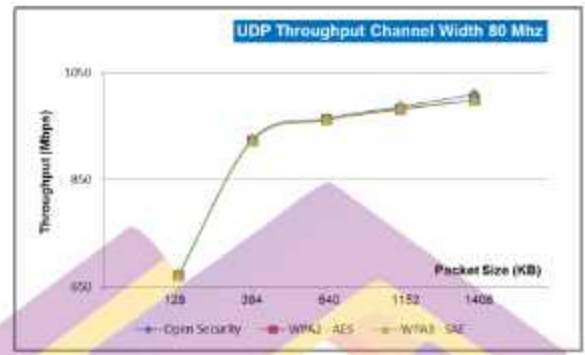


Gambar 4.5 Hasil Pengujian TCP *Throughput Channel Width* 80 Mhz

Pada penggunaan *channel width* 80 Mhz, hasil pengujian protokol TCP menunjukan bahwa penggunaan *wireless security protocol* baik WPA2 – AES maupun WPA3 – SAE mengalami penurunan bila dibandingkan ketika jaringan *wireless* tidak menerapkan *wireless security protocol* (*Open Security*).

Namun pada penggunaan WPA3 – SAE lebih baik bila dibandingkan dengan WPA2 – AES dimana hal ini ditunjukan ketika pengiriman paket sebesar 1408 KB, penggunaan WPA3 - SAE mengalami penurunan *throughput* terbesar adalah 18 Mbps (2,1%) sedangkan untuk penggunaan WPA2 – AES mengalami penurunan hingga 27 Mbps (3,1%).

b. Hasil Pengujian UDP



Gambar 4.6 Hasil Pengujian UDP *Throughput Channel Width* 80 Mhz

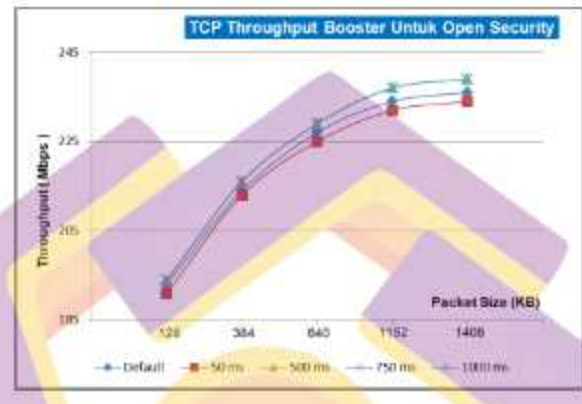
Pada penggunaan *channel width* 80 Mhz, hasil pengujian protokol UDP menunjukan bahwa penggunaan *wireless security protocol* baik WPA2 – AES maupun WPA3 – SAE mengalami penurunan bila dibandingkan ketika jaringan *wireless* tidak menerapkan *wireless security protocol* (*Open Security*).

Namun pada penggunaan WPA3 – SAE lebih baik bila dibandingkan dengan WPA2 – AES. dimana perbedaan penurunan *throughput* dimulai ketika pengiriman paket 384 KB, 640 KB, 1152 KB dan 1408 KB. Untuk WPA3-SAE penurunan terbesar ketika pengiriman paket 1408 KB sebesar 10 Mbps (0,9%) begitu juga untuk WPA2 – AES penurunan terbesar ketika pengiriman paket 1408 KB sebesar 11 Mbps (1,1%).

4.2 Hasil Pengujian Perbandingan Penggunaan *Throughput Booster*

4.2.1 Hasil Pengujian TCP Untuk *Channel Width* 20 Mhz

a. TCP *Throughput Booster* Untuk *Open Security*

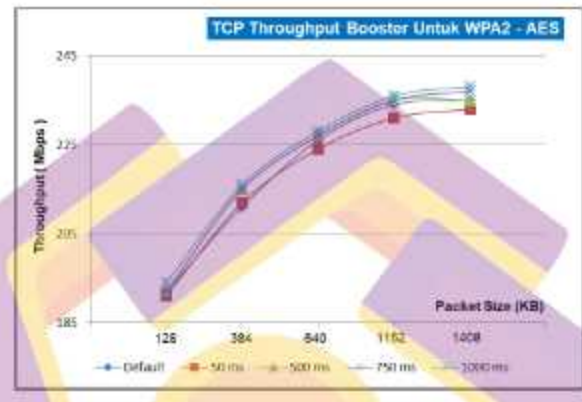


Gambar 4.7 Hasil Pengujian TCP *Throughput Booster* Untuk *Open Security*

Throughput booster merupakan metode yang digunakan untuk meningkatkan kualitas *thoroughput* 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 di atas menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Dimana nilai *default beacon interval* adalah 100 ms, ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 2 Mbps ketika pengiriman paket sebesar 128 KB, 640 KB, 1152 KB dan 1408 KB. Pengujian selanjutnya adalah memberikan nilai *beacon interval*

sebesar 1000 ms, *throughput* yang didapatkan meningkat hingga 3 Mbps ketika pengiriman paket sebesar 1152 KB dan 1408 KB.

b. TCP *Throughput Booster* Untuk WPA2 - AES

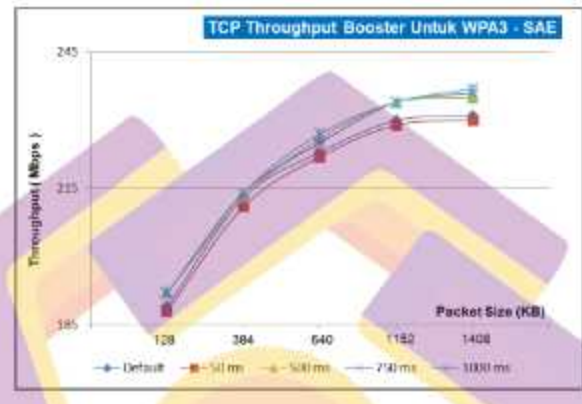


Gambar 4.8 Hasil Pengujian TCP *Throughput Booster* Untuk WPA2-AES

Selanjutnya pada pengujian untuk protokol TCP dengan penggunaan mode WPA2 - AES seperti ditunjukan grafik di atas, sama seperti halnya dengan pengujian untuk mode *open security*, pada mode WPA2 – AES menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Perbandingan *throughput* yang didapatkan ketika nilai *default beacon interval* 100 ms, ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 2 Mbps ketika pengiriman paket sebesar 640 KB, dan 1408 KB. Pengujian selanjutnya adalah memberikan nilai

beacon interval sebesar 1000 ms, *throughput* yang didapatkan meningkat hingga 4 Mbps ketika pengiriman paket sebesar 384 KB.

c. TCP *Throughput Booster* Untuk WPA3 – SAE



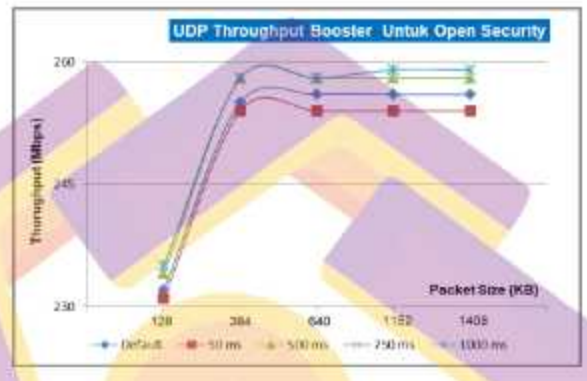
Gambar 4.9 Hasil Pengujian TCP *Throughput Booster* Untuk WPA3-SAE

Selanjutnya pada pengujian untuk protokol TCP dengan penggunaan mode WPA3 - SAE seperti ditunjukan grafik di atas, sama seperti halnya dengan pengujian untuk mode *open security* dan WPA2 – AES, pada mode WPA3 – SAE menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Perbandingan *throughput* yang didapatkan antara nilai *default beacon interval* 100 ms, dengan ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 2 Mbps ketika pengiriman paket sebesar 384 KB. Pengujian selanjutnya adalah dengan memberikan nilai *beacon interval* sebesar 1000 ms, *throughput*

yang didapatkan meningkat hingga 6 Mbps ketika pengiriman paket sebesar 1408 KB.

4.2.2 Hasil Pengujian UDP Untuk *Channel Width* 20 Mhz

a. UDP *Throughput Booster* Untuk *Open Security*

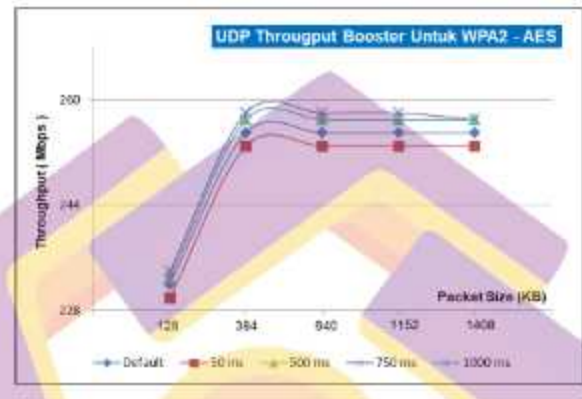


Gambar 4.10. Hasil Pengujian UDP *Throughput Booster* Untuk *Open Security*

Pada pengujian untuk protokol UDP dengan penggunaan mode *Open Security* seperti ditunjukan grafik di atas menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Perbandingan *throughput* yang didapatkan antara nilai *default beacon interval* 100 ms, dengan ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 2 Mbps ketika pengiriman paket sebesar 640 KB, 1152 KB dan 1408 KB. Pengujian selanjutnya adalah memberikan nilai *beacon interval* sebesar 1000 ms, *throughput* yang didapatkan meningkat hingga

3 Mbps ketika pengiriman paket sebesar 128 KB, 384 KB, 1152 KB dan 1408 KB.

b. UDP *Throughput Booster* Untuk WPA2 – AES

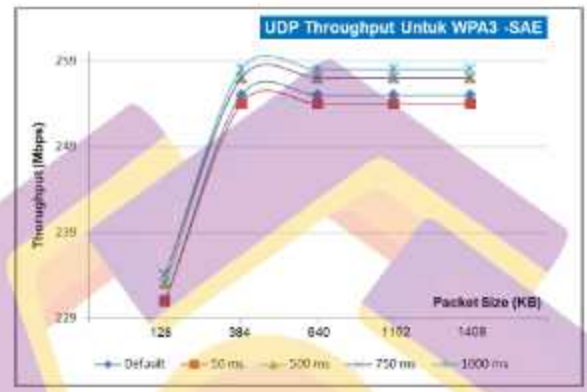


Gambar 4.11. Hasil Pengujian UDP *Throughput Booster* Untuk WPA2 - AES

Selanjutnya pada pengujian untuk protokol UDP dengan penggunaan mode WPA2 - AES seperti ditunjukan grafik di atas, sama seperti halnya dengan pengujian untuk mode *open security*, pada mode WPA2 – AES menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Perbandingan *throughput* yang didapatkan ketika nilai *default beacon interval* 100 ms, ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 2 Mbps ketika pengiriman paket sebesar 128 KB, 384 KB, 640 KB, 1152 KB dan 1408 KB. Pengujian selanjutnya adalah memberikan nilai *beacon interval* sebesar 1000 ms, *throughput* yang

didapatkan meningkat hingga 2 Mbps ketika pengiriman paket sebesar 384 KB, 640 KB, 1152 KB dan 1408 KB.

c. UDP *Throughput Booster* Untuk WPA3 – SAE



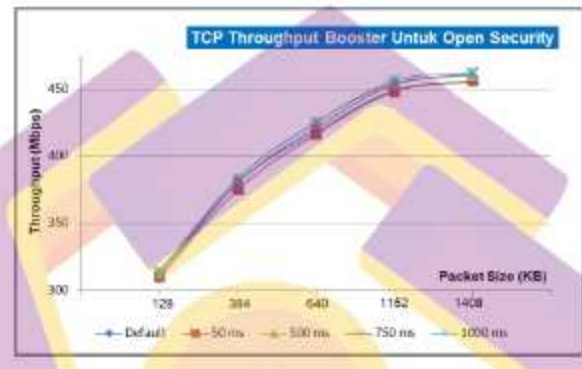
Gambar 4.12. Hasil Pengujian UDP *Throughput Booster* Untuk WPA3 - SAE

Selanjutnya pada pengujian untuk protokol TCP dengan penggunaan mode WPA3 - SAE seperti ditunjukan grafik di atas, sama seperti halnya dengan pengujian untuk mode *open security* dan WPA2 – AES, pada mode WPA3 – SAE menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Perbandingan *throughput* yang didapatkan antara nilai *default beacon interval* 100 ms, dengan ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 1 Mbps ketika pengiriman paket sebesar 384 KB, 640 KB, 1152 KB, dan 1408 KB. Pengujian selanjutnya adalah dengan memberikan nilai *beacon interval*

sebesar 1000 ms, *throughput* yang didapatkan meningkat hingga 3 Mbps ketika pengiriman paket sebesar 128 KB, 384 KB, 640 KB, 1152 KB, dan 1408 KB.

4.2.3 Hasil Pengujian TCP Untuk *Channel Width* 40 Mhz

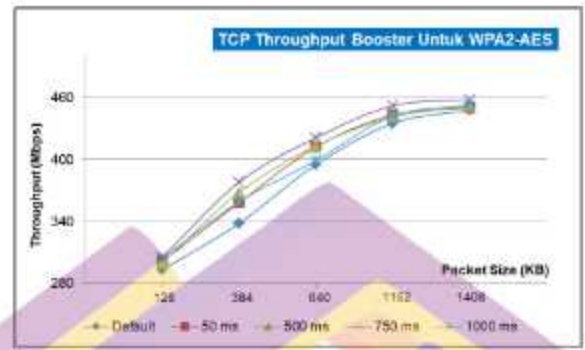
a. TCP *Throughput Booster* Untuk *Open* Security



Gambar 4.13. Hasil Pengujian TCP *Throughput Booster* Untuk *Open Security*

Pada pengujian untuk protokol TCP dengan penggunaan mode *Open Security* di *channel width* 40 Mhz seperti ditunjukan grafik di atas menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Perbandingan *throughput* yang didapatkan antara nilai *default beacon interval* 100 ms, dengan ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 5 Mbps ketika pengiriman paket sebesar 384 KB. Pengujian selanjutnya adalah memberikan nilai *beacon interval* sebesar 1000 ms, *throughput* yang didapatkan meningkat hingga 7 Mbps ketika pengiriman paket sebesar 640 KB, 1152 KB dan 1408 KB.

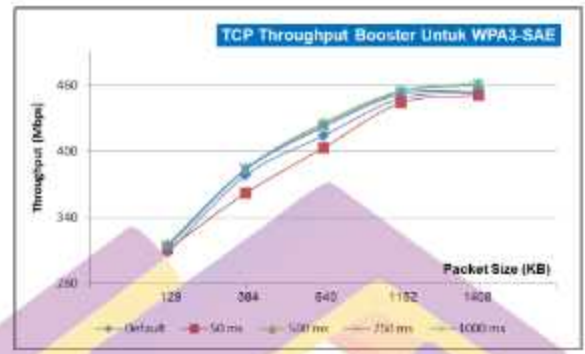
b. TCP *Throughput Booster* Untuk WPA2 – AES



Gambar 4.14. Hasil Pengujian TCP *Throughput Booster* Untuk WPA2-AES

Selanjutnya pada pengujian untuk protokol TCP dengan penggunaan mode WPA2 - AES di *channel width* 40 Mhz seperti ditunjukan grafik di atas menunjukan bahwa penggunaan nilai *beacon interval* maka akan meningkatkan kualitas *throughput* yang dihasilkan. Perbandingan *throughput* tertinggi yang didapatkan adalah ketika mengirimkan paket sebesar 384 KB, dimana pada nilai *beacon interval* 50 ms, *throughput* yang didapatkan meningkat hingga 20 Mbps, kemudian nilai *beacon interval* 500 ms, *throughput* yang didapatkan meningkat hingga 30 Mbps dan ketika nilai *beacon interval* 750 ms, *throughput* yang didapatkan meningkat hingga 40 Mbps. Dari grafik diatas juga menunjukan bahwa untuk *throughput booster* dengan *throughput* tertinggi yang didapatkan ketika menerapkan mode WPA2 – AES menggunakan nilai *beacon interval* 750 ms, dimana hasilnya ketika mengirimkan paket 128 KB, 384 KB, 640 KB, 1152 KB dan 1408 KB *throughput* yang dihasilkan lebih baik bila dibandingkan dengan nilai *beacon interval* 50 ms, 500 ms dan 1000 ms.

c. TCP *Throughput Booster* Untuk WPA3 – SAE

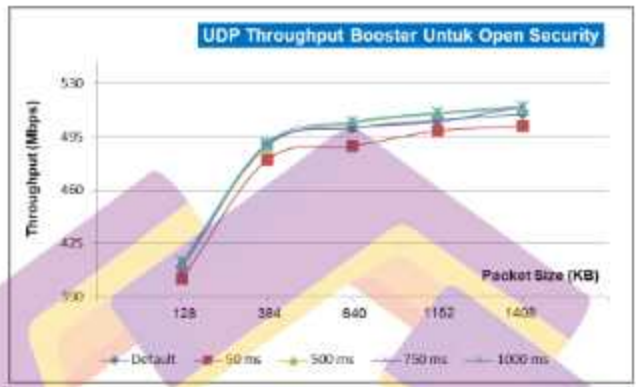


Gambar 4.15. Hasil Pengujian TCP *Throughput Booster* Untuk WPA3-SAE

Selanjutnya pada pengujian untuk protokol TCP dengan penggunaan mode WPA3 - SAE di *channel width* 40 Mhz seperti ditunjukan grafik di atas menunjukan bahwa dengan melakukan perubahan pada nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan menurun. Perbandingan *throughput* yang didapatkan antara nilai *default beacon interval* 100 ms, dengan ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 16 Mbps ketika pengiriman paket sebesar 384 KB. Dari grafik diatas menunjukan juga bahwa nilai beacon interval terbaik untuk mode WPA3 – SAE adalah 500 ms, dimana throughput yang didapatkan meningkat hingga 12 Mbps ketika pengiriman paket sebesar 640 KB.

4.2.4 Hasil Pengujian UDP Untuk *Channel Width* 40 Mhz

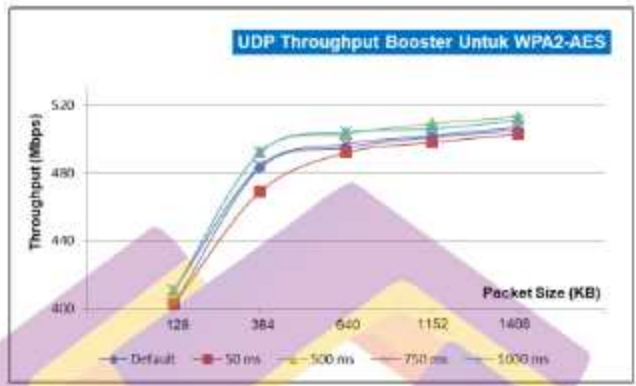
a. UDP *Throughput Booster* Untuk *Open Security*



Gambar 4.16. Hasil Pengujian UDP *Throughput Booster* Untuk *Open Security*

Pada pengujian untuk protokol UDP dengan penggunaan mode *Open Security* di *channel width* 40 Mhz seperti ditunjukan grafik di atas menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Perbandingan *throughput* yang didapatkan antara nilai *default beacon interval* 100 ms, dengan ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 12 Mbps ketika pengiriman paket sebesar 640 KB. Pengujian selanjutnya adalah memberikan nilai *beacon interval* sebesar 1000 ms, *throughput* yang didapatkan meningkat hingga 5 Mbps ketika pengiriman paket sebesar 1152 KB dan 1408 KB.

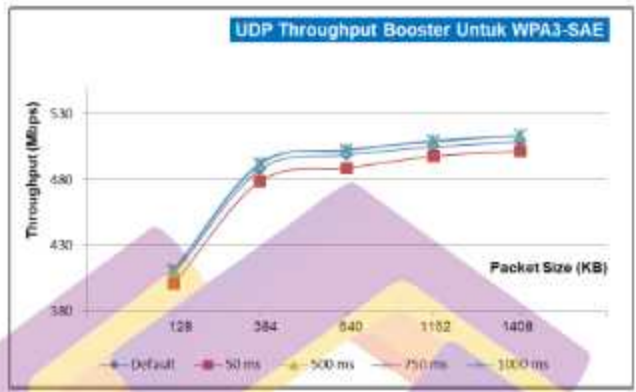
b. UDP *Throughput Booster* Untuk WPA2 – AES



Gambar 4.17. Hasil Pengujian UDP *Throughput Booster* Untuk WPA2 - AES

Selanjutnya pada pengujian untuk protokol UDP dengan penggunaan mode WPA2 - AES di *channel width* 40 Mhz seperti ditunjukan grafik di atas menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Perbandingan *throughput* yang didapatkan antara nilai *default beacon interval* 100 ms, dengan ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 14 Mbps ketika pengiriman paket sebesar 384 KB. Pengujian selanjutnya adalah memberikan nilai *beacon interval* sebesar 1000 ms, *throughput* yang didapatkan meningkat hingga 9 Mbps ketika pengiriman paket sebesar 384 KB dan 640 KB.

c. UDP *Throughput Booster* Untuk WPA3 – SAE

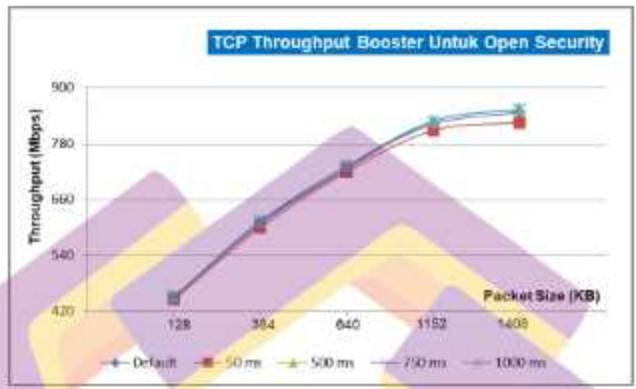


Gambar 4.18. Hasil Pengujian UDP *Throughput Booster* Untuk WPA3 - SAE

Selanjutnya pada pengujian untuk protokol UDP dengan penggunaan mode WPA3 - SAE di *channel width* 40 Mhz seperti ditunjukan grafik di atas menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Perbandingan *throughput* yang didapatkan antara nilai *default beacon interval* 100 ms, dengan ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 10 Mbps ketika pengiriman paket sebesar 640 KB. Pengujian selanjutnya adalah memberikan nilai *beacon interval* sebesar 1000 ms, *throughput* yang didapatkan meningkat hingga 5 Mbps ketika pengiriman paket sebesar 1152 KB dan 1408 KB.

4.2.5 Hasil Pengujian TCP Untuk *Channel Width* 80 Mhz

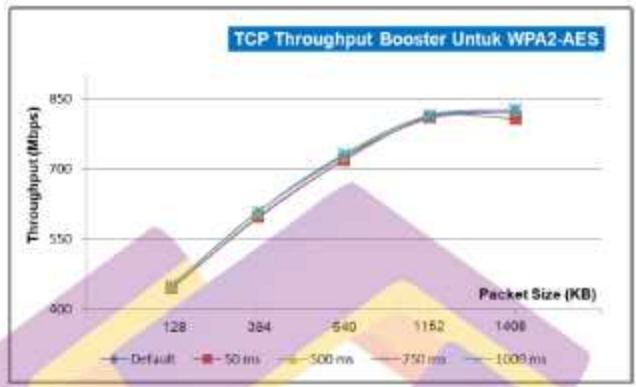
a. TCP *Throughput Booster* Untuk *Open Security*



Gambar 4.19. Hasil Pengujian TCP *Throughput Booster* Untuk *Open Security*

Pada pengujian untuk protokol TCP dengan penggunaan mode *Open Security* di *channel width* 80 Mhz seperti ditunjukan grafik di atas menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Perbandingan *throughput* yang didapatkan antara nilai *default beacon interval* 100 ms, dengan ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 22 Mbps ketika pengiriman paket sebesar 1408 KB. Pengujian selanjutnya adalah memberikan nilai *beacon interval* sebesar 1000 ms, *throughput* yang didapatkan meningkat hingga 7 Mbps ketika pengiriman paket sebesar 1152 KB dan 1408 KB.

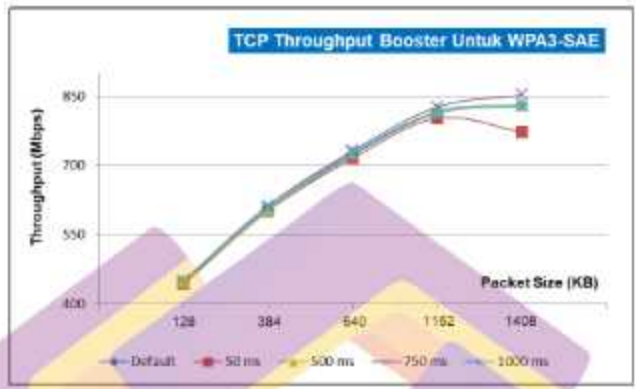
b. TCP *Throughput Booster* Untuk WPA2 – AES



Gambar 4.20. Hasil Pengujian TCP *Throughput Booster* Untuk WPA2-AES

Selanjutnya pada pengujian untuk protokol TCP dengan penggunaan mode WPA2 - AES di *channel width* 80 Mhz seperti ditunjukan grafik di atas menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Perbandingan *throughput* yang didapatkan antara nilai *default beacon interval* 100 ms, dengan ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 14 Mbps ketika pengiriman paket sebesar 1408 KB. Pengujian selanjutnya adalah memberikan nilai *beacon interval* sebesar 1000 ms, *throughput* yang didapatkan meningkat hingga 13 Mbps ketika pengiriman paket sebesar 384 KB dan 640 KB.

c. TCP *Throughput Booster* Untuk WPA3 – SAE

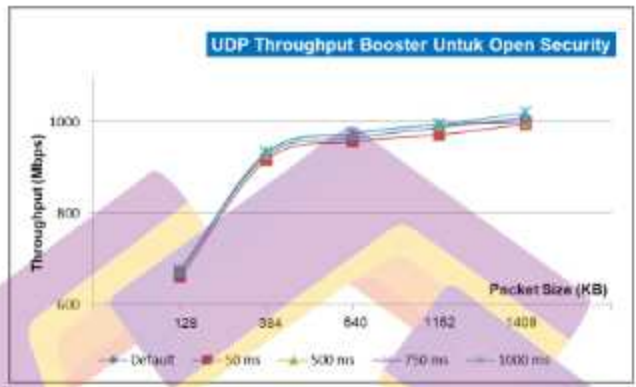


Gambar 4.21. Hasil Pengujian TCP *Throughput Booster* Untuk WPA3-SAE

Selanjutnya pada pengujian untuk protokol TCP dengan penggunaan mode WPA3 - SAE di *channel width* 80 Mhz seperti ditunjukan grafik di atas menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Perbandingan *throughput* yang didapatkan antara nilai *default beacon interval* 100 ms, dengan ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 57 Mbps ketika pengiriman paket sebesar 1408 KB. Dari grafik di atas juga menunjukan bahwa untuk nilai *beacon interval* terbaik adalah 750 ms dimana *throughput* yang dihasilkan meningkat hingga 23 Mbps ketika pengiriman paket sebesar 1408 KB.

4.2.6 Hasil Pengujian UDP Untuk *Channel Width* 80 Mhz

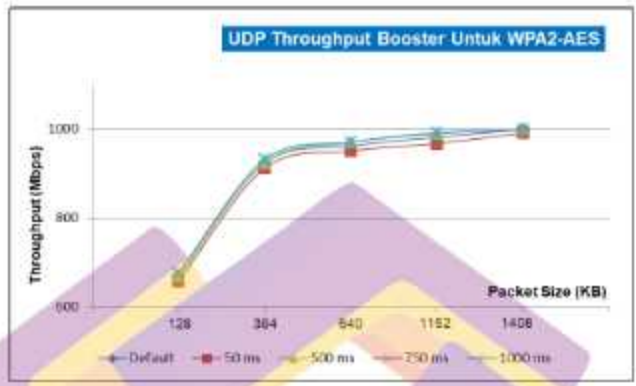
a. UDP *Throughput Booster* Untuk *Open Security*



Gambar 4.22. Hasil Pengujian UDP *Throughput Booster* Untuk *Open Security*

Pada pengujian untuk protokol UDP dengan penggunaan mode *Open Security* di *channel width* 80 Mhz seperti ditunjukan grafik di atas menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Perbandingan *throughput* yang didapatkan antara nilai *default beacon interval* 100 ms, dengan ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 15 Mbps ketika pengiriman paket sebesar 1408 KB. Pengujian selanjutnya adalah memberikan nilai *beacon interval* sebesar 1000 ms, *throughput* yang didapatkan meningkat hingga 10 Mbps ketika pengiriman paket sebesar 640 KB dan 1408 KB.

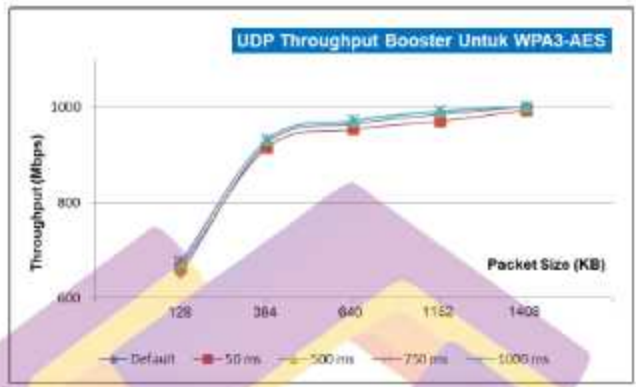
b. UDP *Throughput Booster* Untuk WPA2 – AES



Gambar 4.23. Hasil Pengujian UDP *Throughput Booster* Untuk WPA2 - AES

Pada pengujian untuk protokol UDP dengan penggunaan mode WPA2 - AES di *channel width* 80 Mhz seperti ditunjukan grafik di atas menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Perbandingan *throughput* yang didapatkan antara nilai *default beacon interval* 100 ms, dengan ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 14 Mbps ketika pengiriman paket sebesar 1152 KB. Pengujian selanjutnya adalah memberikan nilai *beacon interval* sebesar 1000 ms, *throughput* yang didapatkan meningkat hingga 10 Mbps ketika pengiriman paket sebesar 1152 KB.

c. UDP *Throughput Booster* Untuk WPA3 – SAE



Gambar 4.24. Hasil Pengujian UDP *Throughput Booster* Untuk WPA3 - SAE

Pada pengujian untuk protokol UDP dengan penggunaan mode WPA3 - SAE di *channel width* 80 Mhz seperti ditunjukan grafik di atas menunjukan bahwa semakin besar penggunaan nilai *beacon interval* maka kualitas *throughput* yang dihasilkan juga akan semakin meningkat, begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun. Perbandingan *throughput* yang didapatkan antara nilai *default beacon interval* 100 ms, dengan ketika pengujian diberikan nilai *beacon interval* 50 ms, *throughput* yang didapatkan menurun hingga 14 Mbps ketika pengiriman paket sebesar 1152 KB. Pengujian selanjutnya adalah memberikan nilai *beacon interval* sebesar 1000 ms, *throughput* yang didapatkan meningkat hingga 24 Mbps ketika pengiriman paket sebesar 128 KB.

4.3 Pembahasan Hasil Penelitian

Hasil pengujian telah dilakukan dengan dua tahap yaitu pada tahap pertama adalah untuk mengetahui dampak penggunaan *wireless security protocol* terhadap *throughput* yang didapatkan oleh PC *Client* dan pada tahap kedua adalah untuk mengetahui dampak penggunaan *beacon interval* untuk meningkatkan *throughput* ketika menerapkan *wireless security protocol*.

4.3.1 Metrik Kinerja Jaringan

Topologi pengujian telah dijelaskan di dalam bab sebelumnya, dimana menggunakan topologi *client server* yang terhubung melalui jaringan *wireless* IEEE 802.11ax. Penggunaan tiga *wireless security protocol open security*, WPA2-AES dan WPA3-SAE dan *beacon interval* sebagai ukuran kinerja yang dapat menghasilkan *throughput* tertinggi ketika digunakan di *channel width* 20 Mhz, 40 Mhz, dan 80 Mhz. Pengujian masing-masing dilakukan dengan menggunakan dua protokol yaitu TCP dan UDP.

4.3.2 Pengaruh *Wireless Security Protocols* Pada *Throughput*

Throughput merupakan salah satu metrik yang digunakan untuk menganalisa kinerja sebuah jaringan baik jaringan menggunakan media transmisi kabel maupun media transmisi wireless. Seperti pada penjelasan sebelumnya bahwa *throughput* merupakan perhitungan kecepatan (rate) transfer data efektif antara pengirim dan penerima, satuan yang digunakan dalam pengukuran adalah bps (*bit per second*). Pada tahap pengujian ini menggunakan tiga tahap berbeda yaitu ketika jaringan *wireless* IEEE 802.11ax tidak menerapkan *wireless security protocols* (open security) dan ketika menerapkan *wireless security protocols* baik

menggunakan WPA2-AES maupun WPA3-SAE. Hasil pengujian dirangkum ke dalam tabel 4.1 sebagai berikut :

Tabel 4.1. Tabel Hasil Pengujian Pengaruh *Wireless Security Protocols* Pada *Throughput*

Wireless Security Protocols	**Channel Width**					
	20 Mhz		**40 Mhz**		**80 Mhz**	
	TCP	**UDP**	**TCP**	**UDP**	**TCP**	**UDP**
Open Security	236 Mbps	256 Mbps	455 Mbps	510 Mbps	848 Mbps	1010 Mbps
WPA2-AES	235 Mbps	255 Mbps	448 Mbps	505 Mbps	821 Mbps	999 Mbps
WPA3-SAE	231 Mbps	255 Mbps	453 Mbps	509 Mbps	830 Mbps	1000 Mbps

Dari tabel 4.1 dapat disimpulkan bahwa *throughput* tertinggi dihasilkan ketika jaringan *wireless* IEEE 802.11ax tidak menerapkan *wireless security protocol* (menggunakan mode open security) baik untuk *channel width* 20 Mhz, 40 Mhz dan 80 Mhz. Hal ini juga menunjukan bahwa dengan mengaktifkan *wireless security protokol* maka *throughput* yang didapatkan akan mengalami penurunan, sebagai contoh untuk pengujian protokol TCP dengan *channel width* 20 Mhz penggunaan WPA2-AES mengalami penurunan 0.4% dan WPA3-SAE mengalami penurunan 2.1%. Selanjutnya untuk *channel width* 40 Mhz

penggunaan WPA2-AES mengalami penurunan 1.5% dan WPA3-SAE mengalami penurunan 0.4%. Dan untuk *channel width* 80 Mhz penggunaan WPA2-AES mengalami penurunan 3.2% dan WPA3-SAE mengalami penurunan 2.1%.

Beberapa penelitian terkait dampak penggunaan *wireless security protocols* terhadap kualitas *throughput* telah banyak dilakukan dengan standar *wireless* IEEE 802.11 g/n/ac akan tetapi masih sedikit penelitian dengan standar *wireless* IEEE 802.11ax. Beberapa penelitian yang telah dilakukan dirangkum sebagai berikut :

1. Pada penelitian yang telah dilakukan oleh (Barka and Boulmalf 2007) menggunakan standar *wireless* IEEE 802.11g membuktikan bahwa *throughput* mengalami penurunan ketika menerapkan *wireless security protocols* baik WEP dan WPA.
2. Pada penelitian yang telah dilakukan oleh (Narayan et al. 2009) menggunakan standar *wireless* IEEE 802.11n dengan topologi pengujian *client server* dan variasi penggunaan empat sistem operasi yaitu Windows XP, Vista, Server 2008 dan Ubuntu menunjukan bahwa penurunan *throughput* mengalami penurunan ketika menerapkan *wireless security protocols* WEP-64, WEP-128, WPA dan WPA2.
3. Pada penelitian yang telah dilakukan oleh (Hayajneh et al. 2012) menggunakan standar *wireless* IEEE 802.11n mebuktikan bahwa *throughput* mengalami penurunan ketika menerapkan *wireless security protocols* untuk

penggunaan aplikasi multimedia baik ketika menerapkan WEP, WPA dan WPA2.

4. Pada penelitian yang dilakukan oleh (Samad Salehi Kolahi et al. 2009) menggunakan standar *wireless* IEEE 802.11n, Tujuan utama dari penelitian ini adalah untuk menganalisis dampak penggunaan protokol keamanan WPA2 pada *throughput* untuk sistem operasi yang berbeda. Hasil penelitian menyimpulkan bahwa terjadi penurunan *throughput* untuk kedua versi IP di ketika menerapkan WPA2.Namun bila dibandingkan dengan IPv6, penurunan pada IPv4 lebih rendah.
5. Pada penelitian yang telah dilakukan oleh (Mohammed 2016) menunjukkan bahwa kualitas *throughput* data yang dihasilkan ketika jaringan *wireless* tidak menerapkan sistem keamanan hasilnya lebih tinggi dibandingkan ketika sistem keamanan diterapkan di dalam jaringan *wireless*. 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).

Bila dibandingkan dengan penelitian sebelumnya yang menggunakan standar *wireless* 802.11 g/n/ac, pada penelitian yang dilakukan dalam tesis ini juga memiliki hasil yang sama yaitu terjadinya penurunan *throughput* ketika menggunakan *wireless security protocols* baik WPA2-AES maupun WPA3-SAE pada jaringan *wireless* IEEE 802.11ax. Hasil penelitian juga menunjukan penggunaan *open security* dengan protokol UDP menghasilkan *throughput* tertinggi baik pada *channel width* 20 Mhz, 40 Mhz dan 80 Mhz.

Pada penggunaan WPA2-AES mengalami penurunan lebih besar bila dibandingkan dengan WPA3-SAE, hal ini dikarenakan pada WPA2-AES menggunakan metode kriptografi AES 128 bit yang membutuhkan waktu lebih lama dalam penulisan dan pembacaan data, dimana waktu yang dibutuhkan akan semakin besar seiring dengan bertambahnya panjang data yang diproses (Ratnadewi et al. 2017) dan rumitnya langkah proses di dalam kriptografi AES tersebut (Pendli et al. 2016), sehingga memberikan dampak pada *throughput* yang didapatkan. Hal ini terlihat jelas ketika penggunaan di *channel width* 40 Mhz dan 80 Mhz dimana pada *channel width* ini jumlah data yang dikirimkan dari PC *client* ke PC *server* memiliki jumlah data yang besar sehingga berdampak pada penurunan *throughput* yang semakin besar ketika menerapkan WPA2-AES bila dibandingkan ketika penggunaan WPA3-SAE. Selanjutnya penurunan *throughput* juga disebabkan oleh mekanisme waktu proses *passphrase*, seperti yang telah dikemukakan (Panizza n.d.) dimana di dalam penelitiannya menunjukan bahwa WPA3-SAE memiliki mekanisme waktu proses *passphrase* lebih cepat yaitu dilakukan hanya satu kali sedangkan pada WPA2-Personal (TKIP dan AES) dilakukan dua kali.

4.3.3 Pengaruh Penggunaan *Beacon Interval* Pada *Throughput*

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 (Pratama et al. 2017). Pada pengujian tahap kedua ini

adalah untuk mengetahui dampak penggunaan *beacon interval* untuk meningkatkan *throughput* ketika menerapkan *wireless security protocol*. Tahap pengujian kedua ini terdiri dari tiga skenario pengujian, dimana pada masing-masing skenario menerapkan WPA2-AES dan WPA3-SAE. Sebagai contoh untuk hasil pengujian protocol TCP dirangkum ke dalam tabel 4.2 sebagai berikut :

Tabel 4.2. Tabel Hasil Pengujian Pengaruh *Beacon Interval* Pada *Throughput*

Channel Width 20 Mhz					
Wireless Security Protocol	**Beacon Interval (ms)**				
	Default (100)	**50**	**500**	**750**	**1000**
WPA2-AES	235 Mbps	233 Mbps	235 Mbps	237 Mbps	238 Mbps
WPA3-SAE	231 Mbps	230 Mbps	235 Mbps	236 Mbps	237 Mbps
Channel Width 40 Mhz					
Wireless Security Protocol	**Beacon Interval (ms)**				
	Default (100)	**50**	**500**	**750**	**1000**
WPA2-AES	448 Mbps	450 Mbps	452 Mbps	458 Mbps	453 Mbps

Tabel 4.2. (Lanjutan)

WPA3-SAE	453 Mbps	451 Mbps	462 Mbps	454 Mbps	460 Mbps
Channel Width 80 Mhz					
Wireless Security Protocol	**Beacon Interval (ms)**				
	Default (100)	**50**	**500**	**750**	**1000**
WPA2-AES	821 Mbps	807 Mbps	826 Mbps	822 Mbps	827 Mbps
WPA3-SAE	830 Mbps	773 Mbps	832 Mbps	853 Mbps	829 Mbps

Dari tabel 4.2 dapat disimpulkan bahwa penggunaan nilai *beacon interval* lebih besar dari nilai *default* 100 ms dapat meningkatkan *throughput* yang didapatkan oleh PC *client* di dalam jaringan *wireless* IEEE 802.11ax, hal ini dapat kita lihat pada pengujian di *channel width* 20 Mhz untuk WPA2-AES meningkat hingga 1.3 % dan WPA3-SAE meningkat hingga 2.6 %, kemudian pada pengujian di *channel width* 40 Mhz untuk WPA2-AES meningkat hingga 1.1 % dan WPA3-SAE meningkat hingga 1.5 %, dan pada pengujian di *channel width* 80 Mhz untuk WPA2-AES meningkat hingga 0.7 % dan WPA3-SAE meningkat hingga 2.8 %.

Hasil penelitian di dalam tesis ini sama seperti halnya pada penelitian yang telah dilakukan oleh (Sati and Graffi 2015), 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.

Pada penggunaan nilai *beacon interval* yang lebih besar dari nilai *default* dapat mengurangi lalu lintas data yang tidak perlu dalam pemanfaatan saluran jaringan *wireless*, 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 *wireless* sehingga hal ini dapat mengurangi konsumsi energi di *access point* dan meningkatkan ketersediaan *bandwidth*.

BAB V

PENUTUP

5.1. 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 sebagai berikut :

1. Penggunaan jaringan *wireless* 802.11ax memiliki *throughput* maksimal sebesar 1010 Mbps dengan protokol UDP dan 848 Mbps dengan protokol TCP untuk penggunaan di *channel width* 80 Mhz.
2. Penerapan *wireless security protocol* dengan mode WPA2 – AES lebih baik dibandingkan dengan WPA3-SAE untuk penggunaan di *channel width* 20 Mhz, dan untuk penggunaan di *channel width* 40 Mhz penggunaan mode WPA3-SAE lebih baik dibandingkan dengan WPA2-AES begitu juga untuk penggunaan di *channel width* 80 Mhz penggunaan mode WPA3-SAE lebih baik dibandingkan dengan WPA2-AES. Dan berikut adalah Tabel penurunan *throughput* dari hasil pengujian yang telah dilakukan :

Tabel 5.1. Tabel Penurunan *Throughput*

Wireless Security Protocol	Channel Width					
	20 Mhz		40 Mhz		80 Mhz	
	TCP	UDP	TCP	UDP	TCP	UDP
WPA2 - AES	1 Mbps	1 Mbps	23 Mbps	1 Mbps	27 Mbps	10 Mbps
WPA3 - SAE	5 Mbps	1 Mbps	4 Mbps	1 Mbps	18 Mbps	11 Mbps

3. Perubahan nilai pada *beacon interval* dengan nilai yang lebih besar dapat meningkatkan kualitas *throughput* jaringan *wireless* ketika menerapkan *wireless security protocol* baik di *channel width* 20 Mhz, 40 Mhz dan 80 Mhz. begitu juga ketika nilai *beacon interval* semakin kecil maka kualitas *throughput* yang didapatkan juga akan semakin menurun.

5.2. Saran

Saran yang dapat diberikan untuk penelitian selanjutnya adalah diharapkan peneliti selanjutnya dapat melakukan penelitian lebih lanjut terkait dampak *wireless security protocol*, terhadap parameter *Quality of Service* lainnya seperti terhadap kualitas *jitter, packet loss,* dan CPU *utilization* yang didapatkan oleh *client* di dalam jaringan *wireless* 802.11ax.

DAFTAR PUSTAKA

PUSTAKA BUKU

Mulyanta, E.S, 2005. Pengenalan Protokol Jaringan Wireless Komputer, Andi, Yogyakarta

Sofana, Iwan, 2008. Membangun Jaringan Komputer, Informatika, Bandung

Syafrizal, Melwin, 2020. Pengantar Jaringan Komputer, Andi, Yogyakarta

PUSTAKA MAJALAH, JURNAL ILMIAH ATAU PROSIDING

Bakri, Muhammad Amin, Muhammad Farhan, and Aeri Sujatmiko. "Performansi Kinerja Jaringan WLAN 5 GHz Sebagai Alternatif WLAN 2 , 4 GHz Pada Area Perkantoran." 7(2): 53–58.

Bankov, Dmitry, Evgeny Khorov, Andrey Lyakhov, and Sigurd Schelstraete. 2016. "Beacons in Dense Wi-Fi Networks: How to Befriend with Neighbors in the 5G World?" In *WoWMoM 2016 - 17th International Symposium on a World of Wireless, Mobile and Multimedia Networks*,.

Barka, Ezedin, and Mohammed Boulmalf. 2007. "On the Impact of Security on the Performance of WLANs." *Journal of Communications*.

Hayajneh, Thaier, Samer Khasawneh, Bassam Jamil, and Awni Itradat. 2012. "Analyzing the Impact of Security Protocols on Wireless LAN with Multimedia Applications." In *SECURWARE 2012 - 6th International Conference on Emerging Security Information, Systems and Technologies*,.

Kolahi, Samad S., and A. A. Almatrook. 2017. "Impact of Security on Bandwidth and Latency in IEEE 802.11ac Client-to-Server WLAN." *International Conference on Ubiquitous and Future Networks, ICUFN*: 893–97.

Kolahi, Samad S., and Abdulbasit A. Almatrook. 2019. "The Impact of Human Shadowing/Movement on Performance of 802.11ac Client-to-Server WLAN." *International Journal of Computing and Digital Systems* 8(3): 243–51.

Kolahi, Samad S., Shaneel Narayan, Du D.T. Nguyen, and Yonathan Sunarto.

2011. "Performance Monitoring of Various Network Traffic Generators." In *Proceedings - 2011 UKSim 13th International Conference on Modelling and Simulation, UKSim 2011*,.

Kolahi, Samad Salehi, Zhang Qu, Burjiz K. Soorty, and Navneet Chand. 2009. "The Impact of Security on the Performance of IPv4 and IPv6 Using 802.11n Wireless LAN." In *3rd International Conference on New Technologies, Mobility and Security, NTMS 2009*,.

Lepaja, Salem, Arianit Maraj, and Shpat Berzati. 2018. "Wireless LAN Planning and Performance Analysis."

Lepaja, Salem, Arianit Maraj, Iris Efendiu, and Shpat Berzati. 2018. "The Impact of the Security Mechanisms in the Throughput of the WLAN Networks." *2018 7th Mediterranean Conference on Embedded Computing, MECO 2018 - Including ECYPS 2018, Proceedings* (February 2020): 1–5.

Mohammed, Alghamdi Talal. 2016. "Evaluation of WEP , WPA and WPA2 Security Protocols on 802 . 11ac Client to Server WLAN Performance." (9): 1–13.

Narayan, Shaneel, Tao Feng, Xiangle Xu, and Shailaja Ardham. 2009. "Impact of Wireless IEEE802.11n Encryption Methods on Network Performance of Operating Systems." In *2009 2nd International Conference on Emerging Trends in Engineering and Technology, ICETET 2009*,.

Panizza, Jonas. "Identity-Based PSK in WPA2 and WPA3 Networks."

Pendli, Vandan, Mokshitha Pathuri, Subhakar Yandrathi, and Abdul Razaque. 2016. "Improvising Performance of Advanced Encryption Standard Algorithm." In *Proceedings of the 2016 2nd Conference on Mobile and Secure Services, MOBISECSERV 2016*,.

Pratama, Mochamad Adhi et al. 2017. "Throughput Analysis Streaming Service on Wireless Lan 802 . 11N." *e-Proceding of Engineering* 4(3): 3625.

Ratnadewi et al. 2017. "Implementation and Performance Analysis of AES-128 Cryptography Method in an NFC-Based Communication System." *World*

Transactions on Engineering and Technology Education.

Sati, Salem, and Kalman Graffi. 2015. "Adapting the Beacon Interval for Opportunistic Network Communications." In *2015 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2015*,.

Tsetse, Anthony, Emilien Bonniord, Patrick Appiah-Kubi, and Samuel Tweneboah-Kodua. 2018. "Performance Study of the Impact of Security on 802.11ac Networks." *Advances in Intelligent Systems and Computing* 738: 11–17.

PUSTAKA LAPORAN PENELITIAN

Alghamdi, T.M. 2016, Evaluation of WEP, WPA and WPA2 Security Protocols on 802.11ac Client to Server WLAN Performance, Tesis, Master of Computing , Unitec Institute of Technology.

Almatrook, A., 2016, The Effect of Mobility, Security and Shadowing on Latest Wireless LAN Standard (IEEE802.11ac), Tesis, Master of Computing, Unitec Institute of Technology.

Ghanem, M, 2018, IEEE 802.11ac Performance Analysis And Measurement Tools, Tesis, Master of Science in Electrical and Electronic Engineering, University of Oklahoma.

PUSTAKA ELEKTRONIK

Abbas , Ghayyur, 3 April 2021, Transport Layer responsibilities, https://www.geeksforgeeks.org/transport-layer-responsibilities/

Geier, E, 3 April 2021, What is WPA3? And some gotchas to watch out for in this Wi-Fisecurityupgrade, https://www.networkworld.com/article/3316567/what-is-wpa3-wi-fi-security-protocol-strengthens-connections.html

Jain, P; Ashushrma; Rahul Hindocha; Mohitm ; Satya Jitdeb Nath, 3 April 2021, TCP/IP Model, https://www.geeksforgeeks.org/tcp-ip-model/