

Analisa Kinerja Penerapan Standard Protokol Keamanan IEEE 802.11 Pada Layanan Wireless Fidelity

M Zatiar Erwan Kalam¹, Ni Made Ary Dewi Wirastuti², I Made Oka Widyantara³

[Submission:27-01-2021, Accepted: 25-02-2021]

Abstract—Communication networks are increasingly dependent on WLANs, the higher the demands for Quality of Service (QoS) for WLANs such as throughput, delay, jitter and packet loss, to secure data communication media, network security mechanisms are used Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA), and WPA2 [1]. MBG has several alternatives WiFi free, The number of installed Wi-Fi cause problems the interference influence WiFi network performance, MBG has an area indoor and outdoor, alternative to handle the interference is to using the automation channel by applying channel fly, background scanning and static channel. From security mechanisms, channeling and frequency made by doing scenario on carried out research at each access point to get the best scenario, From the scenario proposed, the 5.8 Ghz frequency has better resistance to interference, the results of performance are influenced by interference, the WEP security mechanism has a better packet loss value but produces poor throughput, while WPA and disable security produce good throughput, jitter and delay, channel fly has the best performance but need 30-60 minutes to reach the optimum, while background scanning takes a shorter time but the results obtained are not better than channel fly. On this research scenario 30 AP 1, scenario 16 AP 4, scenario 11 AP 5 and scenario 22 AP 6 have good throughput has good jitter and delay value.

Keywords— QOS, Channeling, Security, Performance

Intisari—Jaringan komunikasi semakin bergantung pada WLAN, maka semakin tinggi tuntutan *Quality of Service (QoS)* WLAN seperti *throughput*, *delay*, dan *jitter* untuk menjaga keamanan media komunikasi data, maka digunakan mekanisme keamanan jaringan *Wired Equivalent Privacy (WEP)*, *WiFi Protected Access (WPA)*, dan *WPA2* [1]. MBG memiliki beberapa alternatif WiFi gratis, Banyaknya *Wi-Fi* yang terpasang menimbulkan permasalahan interferensi yang mempengaruhi unjuk kerja jaringan WiFi, MBG sendiri memiliki area *indoor* dan *outdoor*, alternatif untuk mengatasi interferensi adalah dengan melakukan automasi pengkalan dengan menerapkan *channel fly*, *background scanning* dan *static channel*. Dari mekanisme keamanan, pengkalan dan frekuensi dibuat skenario dilakukan penelitian pada setiap akses point untuk mendapatkan skenario terbaik, dari skenario yang diajukan frekuensi 5.8Ghz memiliki ketahanan lebih baik terhadap interferensi hasil unjuk kerja dipengaruhi oleh interferensi, mekanisme keamanan WEP memiliki nilai *packet*

loss yang lebih baik tetapi menghasilkan *throughput* yang kurang baik sedangkan WPA dan *disable security* menghasilkan *throughput*, *jitter* dan *delay* yang baik, *channeling channel fly* memiliki unjuk kerja terbaik tetapi memerlukan waktu 30-60 menit untuk mencapai optimal sedangkan *background scanning* memerlukan waktu yang lebih singkat tetapi hasil yang diperoleh tidak lebih baik dari *channel fly*. Nilai *throughput* berpengaruh terhadap nilai *delay* dan *jitter*, semakin besar nilai *throughput* nilai *delay* akan semakin baik. pada penelitian yang dilakukan skenario 30 AP 1, skenario 16 AP 4, skenario 11 AP 5 dan skenario 22 AP 6 memiliki nilai *throughput* baik memiliki nilai *jitter* dan *delay* yang baik.

Kata Kunci— QOS, Channeling, Security, Unjuk Kerja

i. PENDAHULUAN

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer, software, dan perangkat jaringan yang bekerja secara bersama. Local Area Network (LAN) merupakan salah satu jenis jaringan komputer yang dapat menghubungkan komputer satu dengan yang lain. Perkembangan teknologi jaringan komunikasi mendapatkan peran penting sebagai media yang dapat menghubungkan antar pengguna tanpa adanya batasan ruang dan waktu. Jaringan komunikasi yang paling dikenal untuk menghubungkan perangkat seluler seperti *smartphone*, *tablet PC*, dan *notebooks* ke internet ialah Wireless Local Area Networks (Wireless LAN/WLAN) [2]. Perkembangan jaringan WLAN saat ini telah mencapai standar 802.11.ac yang berjalan pada frekuensi 2.4 Ghz dan 5.8 Ghz, pada frekuensi 5.8 Ghz dapat mencapai *throughput* 1 Gigabyte (GB) dengan nilai interferensi yang lebih baik dibandingkan dengan frekuensi 2.4 Ghz[3].

Teknologi WLAN menerapkan standar 802.11a/b/g/n/ac dengan frekuensi 2.4 Ghz dan 5.8 Ghz. Guna menjaga keamanan media komunikasi data, maka digunakan mekanisme keamanan jaringan *Wired Equivalent Privacy (WEP)*, *WiFi Protected Access (WPA)*, dan *WPA2*[1]. Jaringan WLAN atau pun LAN yang terhubung pada internet cenderung tidak aman dan bisa di eksploitasi oleh orang yang tidak bertanggung jawab dengan memanfaatkan celah pada proses komunikasi data, data bisa ubah atau diambil untuk mencari keuntungan sendiri[4], walaupun sudah menggunakan WPA2 dan AES sebagai solusi pengamanan tetap memiliki kemungkinan untuk data bisa di curi maka sebagai pengguna internet diharapkan bijak untuk melakukan komunikasi data (*security awareness*)[5].

Permasalahan jaringan WLAN yaitu interferensi bisa diatasi dengan optimasi penggunaan metode *channeling*. Pengkalan pada WLAN berfungsi untuk memperluas saluran serta bersifat statis dan dinamis[6]. Metode *channeling*

¹ Mahasiswa, Magister Manajemen Bisnis Telekomunikasi, Universitas Udayana, Denpasar, Bali, 80232(tlp: 081273226933; e-mail: zatiarasm@yahoo.com)

^{2, 3}Dosen Jurusan Teknik Elektro dan Komputer Fakultas Teknik Universitas Udayana, Jln. Jalan Kampus Bukit Jimbaran 80361 INDONESIA (telp: 0361-703315; fax: 0361-4321; e-mail: dewi.wirastuti@unud.ac.id, e-mail : oka.widyantara@unud.ac.id)



adalah metode *multiple-access* dimana bandwidth yang tersedia dari sebuah link dibagikan berdasarkan waktu, frekuensi atau melalui *coding*. Kekuatan sinyal sangat dipengaruhi oleh *positioning* access point dan *obstacle* yang menjadi pembeda pada area tertentu[7], untuk melindungi keamanan jaringan komunikasi, maka menggunakan jaringan WEP, WPA, dan WPA2, permasalahan tersebut sangat mempengaruhi unjuk kerja dari jaringan WLAN[8].

Mall Bali Galeria adalah mall yang terdapat di kabupaten Badung. MBG memberikan layanan WiFi gratis yang di sediakan oleh ISP yang dapat dengan mudah untuk di akses seperti Bali Fiber, Telkom, dan Biznet, banyaknya Wi-Fi yang terpasang menyebabkan interferensi yang tinggi, hal tersebut dapat mengganggu kualitas dari layanan WiFi MBG. *handover homogeneous* dan *handover heterogeneous* adalah metode perpindahan client dari akses point ke akses point lain dalam satu jaringan yang sama menjadi kelebihan dari teknologi WLAN sekarang membuat *client* tidak perlu terputus dari service yang sedang digunakan[9].

Penelitian yang pernah dilakukan oleh Poonam Jindal dan Brahmjit Singh pada tahun 2015 dengan menghitung mekanisme keamanan sebagai faktor yang mempengaruhi nilai *throughput*[1], pada penelitian yang akan dibahas pada jurnal ini disusun dengan mengkombinasikan mekanisme keamanan (WPA, WEP) dan teknik pengkalan (*static channel*, *channel fly*, *background scanning*) setelahnya akan di analisa faktor-faktor yang mempengaruhi unjuk kerja jaringan WiFi (*throughput*, *jitter*, *delay*, dan *packet loss*), pada skenario penelitian ini akan di kondisikan untuk akses point yang di uji dalam keadaan tanpa beban dan kekuatan sinyal kategori sangat bagus $>-70\text{dBm}$ [10].

II. TINJAUAN PUSTAKA

A. WLAN Standar

Standar yang digunakan pada implementasi jaringan *Wireless Local Area Networks* (WLAN) adalah IEEE 802.11, telah ditentukan semenjak tahun 1997 oleh Institute of Electrical and Electronics Engineers [10]. Dalam keamanan jaringan terdapat beberapa metode untuk menjaga jaringan WLAN menjadi lebih handal dan aman, yaitu dengan menerapkan *firewall* yang handal untuk mengurangi serangan[11], pada jaringan WLAN terdapat metode standar dalam pengamanan jaringan *disable security*, *Wired Equivalent Privacy* (WEP), *WiFi Protected Access* (WPA) dan WPA2[12]. WEP enkripsi menggunakan RC4 dimana 24 bit digunakan untuk inisialisasi *vector iv* dan sisa bit menjadi *secret key*[13].

TABEL I. STANDAR KEAMANAN JARINGAN

	WEP	WPA	WPA2
Year ratified	1999	2003	2004
Key Size [bit]	40	128	128, 192, 256
Key State	Static	Dynamic	Dynamic
Authentication	WEP Key	802.1X&EAP	802.1X&EAP
Encryption	RC4	RC4	AES

B. Throughput

Throughput adalah *bandwidth* aktual yang terukur pada satuan waktu. *Bandwidth* adalah jumlah bit yang bisa dikirim dalam satu detik, *throughput* merupakan indikator utama dari

kualitas jaringan, *throughput* dipengaruhi oleh lebar pita (frekuensi), *bandwidth* yang tersedia, mekanisme keamanan, dan interferensi atau *overlapping channel*, kualitas sinyal juga berpengaruh terhadap unjuk kerja jaringan Wi-Fi, kualitas sinyal dipengaruhi oleh penempatan akses point, *pointing* dan spesifikasi akses point [14].

TABEL II KATEGORI *THROUGHPUT* [10]

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

C. Jitter

Jitter adalah waktu yang diperlukan untuk mengirim data dua arah dari pengirim ke penerima, dan merupakan kumpulan dari semua penundaan yang terjadi dalam proses dari pengiriman data hingga penerimaan data. Faktor-faktor yang mempengaruhi besarnya *jitter* adalah frekuensi, pulsa, amplitudo sinyal atau fase sinyal periodik. Lokasi antara pengguna dan titik akses sangat memengaruhi *jitter*.

TABEL III. JITTER [10]

Degradasi Kategori	Jitter
Perfect	0 ms
Good	75 ms
Medium	125 ms
Poor	225 ms

D. Packet Loss

Packet loss adalah bit yang gagal di transmisikan dari pengirim ke penerima yang menyebabkan hilangnya sebagian data selama proses pengiriman, *collision* menyebabkan paket hilang dan mempengaruhi nilai *packet loss* menggambarkan kondisi jaringan menyebabkan *retransmission* yang mengurangi efisiensi performa jaringan [15].

TABEL IV. PACKET LOSS [10]

Degradasi Kategori	Paket Loss
Perfect	0 %
Good	3 %
Medium	15 %
Poor	25 %

E. Delay

Delay mengacu pada penundaan waktu transmisi paket data dari titik transmisi ke titik lain, selain terhubung untuk melakukan komunikasi *chatting browsing* internet juga dipergunakan untuk membuka *multimedia streaming* yang memiliki karakter tidak toleran terhadap QoS delay [16], ada dua jenis *delay* di jaringan. *packet delay* adalah keterlambatan yang disebabkan oleh waktu yang dibutuhkan pengguna informasi untuk membentuk sebuah paket data IP. Penundaan ini hanya terjadi sekali, pada sumber informasi, *queuing delay* disebabkan oleh waktu proses yang dibutuhkan oleh *router*. *delay* propagasi adalah proses di mana informasi merambat di media transmisi, menyebabkan penundaan yang disebut *delay* propagasi. Kedua, *transmission delay* transmisi adalah waktu

penundaan yang dibutuhkan paket data untuk melintasi media. Penundaan transmisi tergantung pada kecepatan media dan bandwidth yang tersedia[17].

TABLE V. DELAY [10]

Degradasi Kategori	Delay
Perfect	< 150 ms
Good	150 s.d 300 ms
Medium	300 s.d 450 ms
Poor	> 450 ms

F. Signal Strength

Signal strength atau kekuatan sinyal biasa disebut dengan RSSI atau Radio Received Signal Strength Indicator merupakan salah satu faktor yang mempengaruhi nilai dari throughput, kualitas sinyal yang baik bernilai di bawah dari -76dBm[18].

TABEL VI. SIGNAL STRENGTH [10]

RSSI	Sinyal Kategori
>- 70 dBm	Sangat Bagus
-70 dBm sampai -85 dBm	Bagus
-86 dBm sampai -100 dBm	Biasa
<-100 dBm	Buruk
< 110 dBm	Sangat buruk / No signal

G. Metode Channeling

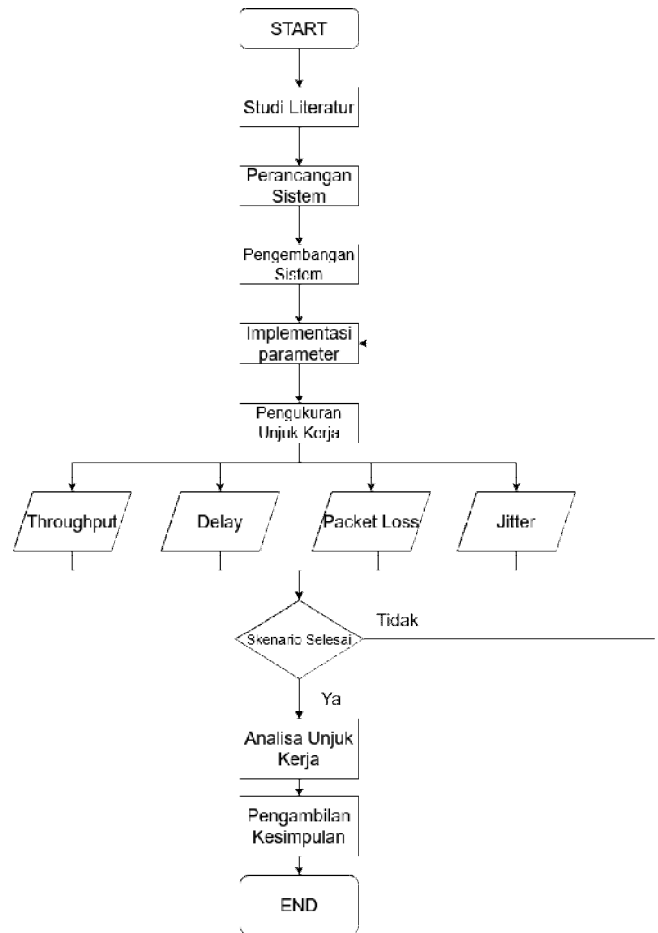
Untuk mengatasi interferensi akses point secara otomatis, beberapa metode yang ditawarkan yaitu metode pemilihan saluran otomatis channel fly dan background scanning. Channel fly untuk pemanfaatan spektrum dan optimalisasi kinerja, sementara background scanning harus diaktifkan untuk mendeteksi AP yang diluar dari manage, deteksi lokasi AP, dan penyesuaian daya radio. Keduanya dapat digunakan untuk optimasi saluran otomatis, perbedaan utama antara channel fly dan background scanning adalah bahwa channel fly menentukan saluran optimal berdasarkan analisis statistik waktu nyata dari pengukuran throughput, sementara background scanning menggunakan pengukuran saluran dan teknik lainnya untuk memperkirakan dampak interferensi pada kapasitas Wi-Fi berdasarkan pemindaian progresif semua saluran yang tersedia, sedangkan untuk static channel adalah menentukan sendiri channel yang digunakan untuk masing-masing akses point[19].

III. METODE PENELITIAN

Penelitian dan pengambilan data dilaksanakan di publik area indoor (hall dan lobby) dan area outdoor (taman dan foodcourt area). Langkah - langkah metode penelitian yang di gunakan dalam penelitian ini seperti pada Gambar 1, studi literatur tahapan di mana penulis mempelajari teori-teori, metode kerja, dan dasar aplikasi dari kasus-kasus yang ada dari jurnal dan buku-buku yang berkaitan dengan permasalahan yang dibahas dalam penelitian ini, perancangan sistem merupakan tahapan untuk mendeskripsikan proses dan parameter (mekanisme keamanan, standar IEEE, teknologi saluran) yang digunakan untuk mendapatkan performansi (jitter, delay, packet loss, dan throughput), pengembangan

M. Z. E. Kalam: Analisa Kinerja Penerapan Standard.....

sistem didasarkan pada analisis desain yang telah diselesaikan sebelumnya untuk menulis rencana pengujian, dan kemudian mengembangkan sistem untuk membuat rencana yang berbeda dengan parameter yang telah ditentukan, implementasi parameter setelah skenario disusun, kemudian ditetapkan sebagai parameter untuk pengujian dan pengukuran selanjutnya untuk mengetahui performa jaringan WLAN, pengukuran unjuk kerja didasarkan pada parameter security, frekuensi, channeling, maka di hasilkanlah jitter, delay, packet loss, dan throughput di ukur sesuai dengan standar tiphon. Tahapan analisa unjuk kerja setelah didapati nilai jitter, delay, packet loss, dan throughput setelahnya di analisis dan di buat kedalam satu tabel untuk bisa diamati unjuk kerja yang terbaik berdasarkan standard tiphon, pengambilan kesimpulan di lakukan setelah menganalisis hasil penelitian yang dilakukan, maka diambil kesimpulan skenario unjuk kerja terbaik jaringan WLAN, kesimpulan yang diambil di tinjau dari rumusan masalah yang telah diidentifikasi dan diselesaikan berdasarkan rancangan dan pengembangan sistem yang telah diimplementasikan.

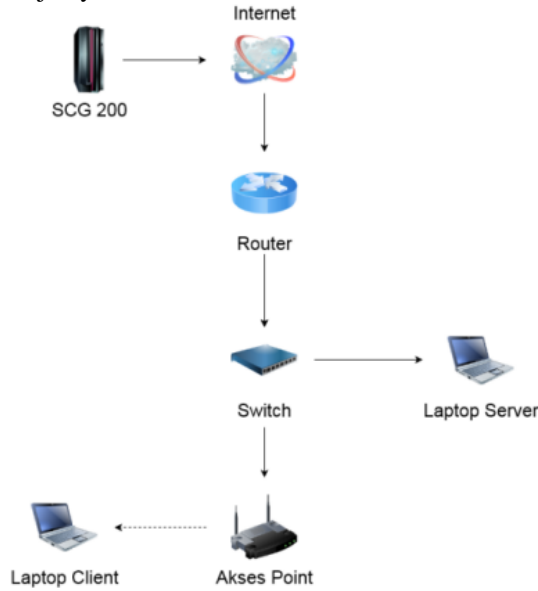


Gambar 1: Flowchart Pengujian

Untuk mendapatkan nilai yang di diharapkan pada Tabel VII skenario pengujian, pengujian akan dilakukan dengan menggunakan 1 laptop yang yang di install iperf3 untuk dijadikan server dan 1 laptop lagi di install Iperf3 sebagai klien saat pengujian laptop server akan dihubungkan



menggunakan kabel UTP cat5e pada posisi *switch* dengan jaringan yang sama dengan akses point, pada posisi pengujian akan dihubungkan menggunakan WiFi melalui akses point yang akan diujikan. Iperf3 akan dijalankan dengan beban yang akan dikirimkan 100Mbps dan protokol UDP dari PC klien ke PC Server untuk selanjutnya diamati dan mengumpulkan data *jitter*, *packet loss*, *delay*, dan *throughput* untuk selanjutnya di analisis.



Gambar 2: Topologi pengujian

Pada pengujian ditentukan skenario dengan mengkombinasikan frekuensi, *security* dan *channeling*, pada skenario pertama akses point R700 *dual band* 2.4Ghz 5.8Ghz, antena *omnidirectional* 3:3x3, upto 1300 Mbps[20], dan T301 *dual band* 2.4Ghz 5.8Ghz, antena *directional* 2x2, upto 867 Mbps[21], dengan akan menjalankan skenario Tabel VII tanpa ada interferensi, pada skenario kedua akses point R700 akan menjalankan skenario Tabel VII pada kondisi interferensi di dalam ruangan, skenario ketiga Akses point T301 menjalankan skenario tabel VII pada kondisi luar ruangan, dari skenario tadi akan dikumpulkan data untuk selanjutnya di analisis.

TABEL VII. SKENARIO PENGUJIAN

Skenario	Security	Channeling	Freq
1	WPA2 - Mixed	Statik Channel	2,4Ghz
2	WPA2	Statik Channel	2,4Ghz
3	WEP-64	Statik Channel	2,4Ghz
4	WEP-128	Statik Channel	2,4Ghz
5	Disable Security	Statik Channel	2,4Ghz
6	WPA2 - Mixed	ChannelFly	2,4Ghz
7	WPA2	ChannelFly	2,4Ghz
8	WEP-64	ChannelFly	2,4Ghz
9	WEP-128	ChannelFly	2,4Ghz
10	Disable Security	ChannelFly	2,4Ghz
11	WPA2 - Mixed	Background Scanning	2,4Ghz
12	WPA2	Background Scanning	2,4Ghz
13	WEP-64	Background Scanning	2,4Ghz

14	WEP-128	Background Scanning	2,4Ghz
15	Disable Security	Background Scanning	2,4Ghz
16	WPA2 - Mixed	Statik Channel	5,8Ghz
17	WPA2	Statik Channel	5,8Ghz
18	WEP-64	Statik Channel	5,8Ghz
19	WEP-128	Statik Channel	5,8Ghz
20	Disable Security	Statik Channel	5,8Ghz
21	WPA2 - Mixed	ChannelFly	5,8Ghz
22	WPA2	ChannelFly	5,8Ghz
23	WEP-64	ChannelFly	5,8Ghz
24	WEP-128	ChannelFly	5,8Ghz
25	Disable Security	ChannelFly	5,8Ghz
26	WPA2 - Mixed	Background Scanning	5,8Ghz
27	WPA2	Background Scanning	5,8Ghz
28	WEP-64	Background Scanning	5,8Ghz
29	WEP-128	Background Scanning	5,8Ghz
30	Disable Security	Background Scanning	5,8Ghz

IV. HASIL DAN PEMBAHASAN

Penelitian ini akan membandingkan hasil analisa unjuk kerja Wi-Fi eksisting dengan *security disable security* dan *channeling channel fly* dengan hasil dari skenario yang diajukan. Pada pengujian skenario *signal strength* yang diujikan dipastikan kategori sangat bagus atau >-70dBm. Untuk perangkat akses point yang di ujikan akan dibuat *iddle* tanpa ada client lain yang terhubung hanya laptop pengujian yang terkoneksi. Beban data yang akan dikirim dari *client* ke *server* sebesar 100Mb dan *bandwidth* dibuat tanpa ada batasan. protokol paket data yang akan diujikan adalah UDP, setiap akses point akan dilakukan pengujian skenario yang sama.

A. Packet Loss

Hasil pengujian skenario diajukan *packet loss* terbaik untuk setiap akses point dengan menggunakan Ruckus R700 dan T301 ditampilkan Tabel VIII AP 1 sampai 4 pada lingkungan ruangan (*hall, ballroom, dan kantin*) dan AP 5 sampai 8 luar ruangan (*park, foodcourt dan play ground*).

TABEL VIII. PACKET LOSS

AP	Skenario	Packet Loss
1	14	1,40%
1	24	0,09%
2	1	0,55%
2	29	0,73%
3	2	0,76%
3	18	0,29%
4	2	0,63%
4	18	0,02%
5	2	0,48%
5	23	0,09%
6	9	1,10%
6	24	0,34%

7	7	0,40%
7	29	0,49%
8	14	0,53%
8	23	0,74%

Pada Tabel VIII setiap akses point memiliki nilai *packet loss* terbaik dengan skenario yang berbeda hal tersebut di pengaruhi oleh interferensi yang terjadi sehingga *packet loss* bervariasi, nilai *packet loss* terbaik didominasi dengan menggunakan *security WEP* dikarenakan penggunaan enkripsi RC4 yang lebih handal untuk mengatasi *packet loss* tetapi memiliki kekurangan pada performa *throughput*, untuk *channeling* penggunaan *channel fly* lebih efektif untuk mengatasi interferensi dan mendapatkan nilai yang lebih baik, berdasarkan Tabel VIII hasil dari *packet loss* nilai *packet loss* yang diperoleh bernilai > 0% sesuai dengan standar tiphon untuk nilai *packet loss perfect* adalah 0 % dan hasil yang didapatkan di atas 0% di bawah 3% kategori *good*.

B. Jitter

Hasil pengujian skenario yang diajukan, *jitter* terbaik untuk setiap akses point dengan menggunakan Ruckus R700 dan Ruckus T301 ditampilkan Tabel IX AP 1 sampai 4 pada lingkungan dalam ruangan (*hall, ballroom, dan kantin*) dan 5 sampai 8 luar ruangan (*taman, foodcourt area dan tempat bermain*).

TABEL IX. JITTER

AP	Skenario	Jitter
1	2	2,665ms
1	30	1,17ms
2	6	1,791ms
2	27	1,336ms
3	5	2,191ms
3	21	1,703ms
4	1	3,815ms
4	16	1,924ms
5	11	3,491ms
5	26	2,163ms
6	12	3,251ms
6	22	1,285ms
7	15	2,958ms
7	30	1,45ms
8	5	1,884ms
8	16	1,116ms

Hasil dari pengujian *jitter* yang ditunjukkan Tabel IX pada setiap akses point terdapat variasi skenario yang menghasilkan nilai *jitter* terbaik karena dipengaruhi oleh interferensi yang terjadi sehingga skenario terbaik bervariasi, *security WPA2* mendominasi nilai *jitter* terbaik, untuk *channeling* penggunaan *background scanning* mendapatkan nilai *jitter* yang baik dikarenakan pada saat pengambilan data dilakukan langsung setelah penerapan skenario tanpa jeda. Berdasarkan Tabel IX hasil dari *jitter* sesuai dengan standar tiphon untuk

M. Z. E. Kalam: Analisa Kinerja Penerapan Standard.....

nilai *jitter perfect* adalah 0 ms dan hasil yang diperoleh > 0ms dibawah 75ms dengan kategori *good*.

C. Delay dan Throughput

Hasil pengujian skenario yang diajukan *throughput* dan *delay* terbaik untuk setiap akses point dengan menggunakan Ruckus R700 dan Ruckus T301 Tabel X AP 1 samapi 4 lingkungan dalam ruangan (*hall, ballroom, dan kantin*) dan 5 sampai 8 luar lingkungan (*taman, foodcourt area dan tempat bermain*).

TABEL X. THROUGHPUT DAN DELAY

AP	Skenario	Delay	Throughput	Eksisting	Optimasi
1	1	21,21ms	39,55 Mbps	33,3 Mbps	19%
1	30	10,65ms	78,7 Mbps	60,7 Mbps	30%
2	5	21,63ms	38,8 Mbps	34,6 Mbps	12%
2	25	14,02ms	59,8 Mbps	59,8 Mbps	0%
3	5	24,24ms	34,6 Mbps	23 Mbps	50%
3	26	11,21ms	74,8 Mbps	47,3 Mbps	58%
4	7	27,68ms	30,3 Mbps	18,7 Mbps	62%
4	16	17,6ms	47,7 Mbps	35,6 Mbps	34%
5	11	28,75ms	28,21 Mbps	14,7 Mbps	92%
5	17	15,67ms	53,5 Mbps	31,3 Mbps	71%
6	15	26,54ms	31,6 Mbps	22,1 Mbps	43%
6	22	11,74ms	71,5 Mbps	49,6 Mbps	44%
7	8	41,7ms	20,1 Mbps	16 Mbps	26%
7	22	11,38ms	73,7 Mbps	65,3 Mbps	13%
8	11	16,43ms	51 Mbps	42,1 Mbps	21%
8	30	10,48ms	80 Mbps	51,6 Mbps	55%

Dari Tabel X bisa dilihat dari skenario yang diajukan bisa meningkatkan performa jaringan WLAN eksisting, untuk mekanisme keamanan WPA2 dan *disable security* menghasilkan nilai *throughput* yang lebih baik jika dibandingkan dengan WEP. Pengkalan *channel fly* dan *background scanning* memiliki performa yang relatif lebih baik dibandingkan pengkalan *static channel*, pengkalan *background scanning* memerlukan waktu yang lebih cepat untuk meningkatkan performa hasil yang di peroleh tidak lebih baik dari *channel fly* tetapi memerlukan waktu yang lebih lama 30 - 60 menit untuk mendapatkan *channel* dengan performa terbaik sebelum dilakukan pengambilan data. Dari Tabel X hasil *throughput* tersebut di pengaruhi oleh interferensi yang terjadi sehingga *throughput* bervariasi, skenario yang diajukan mendapatkan peningkatan performa dari skenario eksisting sesuai dengan standar tiphon untuk nilai *throughput perfect* 100% dan hasil yang didapatkan diatas 25% dibawah 100%.

V. KESIMPULAN

Berdasarkan observasi hasil penelitian yang telah dilakukan di MBG, analisa pembahasan mekanisme keamanan dan pengkalan berdampak pada *Quality Of Service (jitter, packet loss, throughput, delay)* serta unjuk kerja dari performa

p-ISSN:1693 – 2951; e-ISSN: 2503-2372



jaringan WLAN di MBG dapat ditarik kesimpulan dari skenario yang diajukan skenario terbaik untuk area dalam ruangan dan luar ruangan mekanisme keamanan WEP menghasilkan nilai *packet loss* yang lebih baik tetapi menghasilkan nilai *throughput*, *delay* dan *jitter* yang kurang baik dibandingkan dengan WPA dan *disable security*. Besaran nilai *throughput* berpengaruh terhadap nilai *delay* dan *jitter*, semakin besar nilai *throughput* nilai *delay* dan *jitter* akan semakin baik. Pada penelitian yang dilakukan, skenario 30 AP 1, skenario 16 AP 4, skenario 11 AP 5 dan skenario 22 AP 6 memiliki nilai *throughput* baik memiliki nilai *jitter* dan *delay* yang baik. Frekuensi 5 Ghz menunjukan unjuk kerja yang lebih baik dibandingkan 2.4Ghz, frekuensi 5Ghz memiliki lebar band yang lebih lebar dan lebih tahan terhadap interferensi dari sinyal radio lain *Channel fly* memiliki nilai performa terbaik dalam implementasi pengkalan tetapi *channel fly* memerlukan waktu yang relatif lebih lama (30-60 menit) untuk mendapatkan performa yang optimal, sedangkan *background scanning* memerlukan waktu yang lebih cepat untuk meningkatkan nilai performa dari yang sebelumnya, tetapi nilai performa yang diperoleh tidak lebih baik dari *channel fly*, pergeseran *channel* terjadi setiap 15 detik sampai mendapatkan performa yang baik jika terdapat interferensi dikarenakan akses point lain yang melakukan pergeseran *channel* maka akses point tersebut melakukan pergeseran kembali.

REFERENSI

- [1] U. Singh and P. Jindal, "Performance Analysis of Secure Wireless Local Area Network using Test-bed," 2014 Fourth International Conference on Advanced Computing & Communication Technologies. 2014.
- [2] K. C. Hu, S. W. Wang, M. C. Chiang, and C. W. Tsai, "An efficient hybrid algorithm for balancing the load of wireless local area network," Computers and Electrical Engineering (2016). <http://dx.doi.org/10.1016/j.compeleceng.2016.09.036>. 2016.
- [3] T. A. T. Aziz, M. R. A. Razak, and N. E. A. Ghani, "The Performance of Different IEEE802.11 Security Protocol Standard on 2.4GHz and 5GHz WLAN Networks," International Conference on Engineering Technology and Technopreneurship (ICE2T). 2017.
- [4] B. A. Nugroho, H. Supriyono and J. Wantoro, "Analisis Keamanan Jaringan pada Fasilitas Internet (WiFi) Terhadap Serangan Packet Snifing," 2012.
- [5] S. Zaim, "Apakah WPA/WPA2 Benar-Benar Aman? Deskripsi Paket Data Terenkripsi Pada WPA/WPA2," Seminar Nasional Informatika, 2015 (semnasIF 2015), 2015.
- [6] O. Bejarno, and E. W. Knightly, "IEEE 802.11ac: From Channelization to Multi-User MIMO," Rice UniversityMinyoung Park, Intel Corporation. 2013.
- [7] P. D. Pradnyana, D. M. Wiharta, and N. P. Sastra, "Analisis Cakupan Layanan Wi-Fi Gedung Pascasarjana Universitas Udayana," Jurnal SPEKTRUM Vol. 6, No. 2 Juni 2019. 2019.
- [8] Handdy I. G. M, Diafari I. G. A. K, and Indra N, "Pemanfaatan Media Sosial Sebagai Otentifikasi dan Otorisasi Akses ke Jaringan WiFi" E-Jurnal SPEKTRUM Vol. 3, No.2 Desember 2016. 2016.
- [9] N. M. A. E. D. Wirastuti and C. C. W. Emehel, "Handover Scenarios for Mobile WiMAX and Wireless LAN Heterogeneous Network," Telkonnika Indonesian Journal Electrical Engineering, Vol. 12, No. 8., 2014.
- [10] Telecommunications and internet Protocol Harmoniza Over Networks (TIPHON), General aspect of Quality of Service (QOS), Tiphon 1999.
- [11] A. Maraj, G.Jakupi, E. Rogova and X.Grajqevci, "Testing of Network Security Systems Through DoS Attacks," 6th Mediterranean Conference on Embedded Computing. 2017.
- [12] S. Lepaja, A. Maraj, A. Efendiu, and S. Berzati, "The Impact of the Security Mechanisms in the Throughput of the WLAN Networks," 7th Mediterranean Conference on Embedded Computing. 2018.
- [13] E. Barka, M. Boulmalf, A. A. H. A. Suwaidi, H. Khazaimy, and M. A. Mansouri, "Impact of Security on the Performance of Wireless-Local Area Networks," 2006
- [14] K. Y. Krisnawan, N. P. Sastra, and N. M. A. E. D. Wirastuti, "Optimasi Nirkabel Local Area Networks Fakultas Teknik Kampus Sudirman Universitas Udayana," E-Jurnal SPEKTRUM Vol. 5, No 1 Juni 2018. 2018.
- [15] Linawati, N. Gunantara and I. K. A. R. Gunawan, "Performansi WLAN Kantor Pusat Pemerintahan Kabupaten Badung," Teknologi Elektro., Vol.14, No.2, 2015.
- [16] I. M. O. Widyantara, B. D. Cahyono and W. Setiawan, "Analisa Horizontal Handover Terhadap QoS Layanan Streaming Multimedia E-Learning Pada Jaringan WLAN 802.11," Jurnal Teknologi Elektro., Vol.14, No.1, 2015.
- [17] R. Murty, J. Padhye, R. Chandra, A. Wolman, and B. Zill, "Designing High Performance Enterprise Wi-Fi Networks, ". Harvard University, Microsoft Research. 2008.
- [18] S. Jeon, Y. S. Shim, and S.Park, "Study of the Throughput of WLAN According to Channeling and Density of AP," 19th International Conference on Microwaves, Radar & Wireless Communications. 2012
- [19] "Background Scanning and Channel Fly." [Online]. Available: <https://docs.ruckuswireless.com/unleashed/200.1.9.12/c-SelfHealing.html>. [Accessed: 10-December-2020].
- [20] "Data Sheet Ruckus ZoneFlex R700." [Online]. Available: <https://www.ruckusecurity.com/ZoneFlex-R700.asp>. [Accessed: 10-December-2020].
- [21] "Data Sheet Ruckus ZoneFlex T301." [Online]. Available: <https://www.ruckusecurity.com/ZoneFlex-T301.asp>. [Accessed: 10-December-2020].