Prosiding Seminar Nasional SMIPT 2020
Sinergitas Multidisiplin Ilmu Pengetahuan dan Teknologi, vol. 3, nol. 1, 2020
p-ISSN: 2622-0520; e-ISSN: 2622-593X

Serangan Sinyal Jamming Menggunakan Wemos D1 Mini Pada Wireless IEEE 802.11i

Ahmad Suwardi[1], Berkat Fa'atulo Halawa[2], Robby Toro[3], Rahmalia Syahputri[4]
[1-4]*Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Institut Informatika & Bisnis Darmajaya*

Corresponding Author:Ahmad Suwardi
Penulis Pertama: Telp: 085384481903
E-mail: ahmadsuwardi.1711010173@mail.darmajaya.ac.id

Abstrak: Pemanfaatan jaringan nirkabel di masa pandemic COVID-19 saat ini sangat tinggi untuk menunjang pendidikan, pekerjaan, dan lainnya. Jaringan nirkabel memanfaatkan gelombang elektromagnetik yang mempunyai besaran energi listrik serta magnet tanpa membutuhkan media rambat kabel. Jaringan nirkabel seperti wireless local area network (WLAN), disebut juga sebagai Wi-Fi, menggunakan teknologi WPA2-PSK untuk keamanan komunikasi. Teknologi tersebut menerapkan algoritma AES dan CCMP untuk menggantikan teknologi TKIP yang digunakan pada versi WPA sebelumnya. Pada sistem keamanan jaringan WPA2-PSK, penyerang dapat menggunakan gelombang radio sebagai media untuk mengacaukan hingga mematikan koneksi jaringan pada accsess point. Serangan sinyal jamming ini menyebabkan wireless kehilangan kemampuan untuk memberikan layanan kepada perangkat lain (*denial of service)*. Untuk mengetahui jenis serangan sinyal jamming dan waktu yang dibutuhkan untuk mematikan fungsi accesss point telah di bangun simulasi serangan sinyal jamming berdasarkan tiga jarak yang berbeda dari perangkat penyerang yang menggunakan wemos d1 mini ke acces point. Berdasarkan simulasi tersebut, jarak dan kekuatan sinyal unduh dan unggah sangat berpengaruh pada proses jamming yang dilakukan. Semakin dekat jarak penyerang pada accesss point dan semakin besar kekuatan sinyal, maka akan semakin lama waktu yang diperlukan untuk mematikan fungsi accesss point.

Kata Kunci: Sinyal Jamming, Wireless, Password, WPA2-PSK, IEEE

1. PENDAHULUAN

Pada masa pandemic COVID-19 saat ini, banyak sekali kebijakan yang ditetapkan oleh Pemerintah terutama dibidang pendidikan antara lain penerapan sekolah dari rumah. Kebijakan ini berimbas, salah satunya, pada penggunaan teknologi jaringan nirkabel yang sangat tinggi. Teknologi nirkabel (wireless) memenuhi ragam keperluan dari komunikasi jarak dekat dan spontanitas yang difasilitasi oleh perangkat bluetooth hingga jarak jauh seperti menjembatani komunikasi data antar negara melalui teknologi telpon selular.

Teknologi wireless yang sangat popular penggunaannya saat ini antara lain adalah wireless local area network (WLAN).

Walaupun terdapat banyak kelebihan dari implementasi teknologi Wi-Fi, ternyata teknologi ini mempunyai banyak celah kelemahan dalam keamanan dibanding dengan jaringan menggunakan kabel. Jaringan yang menggunakan kabel hanya meliputi penanganan pada komputer yang terhubung dengan jaringan tersebut, beda halnya dengan jaringan yang menggunakan teknologi Wi-Fi yang cakupan jangkauan lebih luas dan bisa digunakan di mana saja yang memungkinkan pengguna jaringan wireless untuk masuk atau menggunakan fasilitas Wi-Fi atau bahkan mengambil data-data pengguna Wi-Fi lainnya yang terhubung di dalam satu jaringan lokal untuk kepentingan tertentu. Teknologi jaringan wireless seperti Wi-Fi ini rentan terhadap berbagai macam serangan, salah satu di antaranya adalah serangan jamming (3)

Jamming merupakan proses atau metode untuk melumpuhkan komunikasi elektronik dengan cara menimpa atau menutupi sinyal dari suatu pemancar dengan sinyal lain (disebut sinyal jamming) yang mempunyai frekuensi sama dengan pemancar tetapi

**Corresponding Author: Ahmad Suwardi Pertama Email: ahmadsuwardi.1711010173@mail.darmajaya.ac.id*

***Article History**: Received: September 02, 2019, Accepted: Oktober 01, 2020*

mempunyai daya atau energi yang lebih besar, sehingga penerima hanya akan mendeteksi sinyal jamming. Pemutus, pengacak, dan pemblok sinyal adalah alat yng digunakan sebagai alat penghilang sinyal. Jammer adalah suatu perangkat elektronik yang berfungsi untuk melumpuhkan komunikasi elektronik yang menggunakan frekuensi radio sebagai media pengiriman informasinya [1].

Jamming adalah jenis serangan yang cukup mudah dengan memanfaatkan single node (baik ground station ataupun pesawat) atau area dengan lebih dari satu node untuk membuat tidak berfungsinya node tersebut, akan mengirim dan menerima ADS-B message dengan cara mengirim signal menggunakan daya yang relatif besar di 1090MHz frequency pada Mode S [5]

Setiap perangkat yang memiliki wireless adapter dapat mendeteksi sinyal wireless yang ada di sekitar cakupannya. Hal ini berarti Wi-Fi memiliki keamanan yang rentan terhadap serangan jika setiap pengguna terhubung dalam satu jaringan dan hanya menggunakan autentikasi berupa password. Terdapat celah pada sisi pengguna yang dapat dipergunakan oleh hacker untuk masuk ke dalam jaringan yang sama, sehingga penyerang dapat mencuri data para pengguna yang terhubung ke jaringan tersebut.

Wi-Fi memanfaatkan gelombang radio dalam frekuensi yang telah di miliki oleh masyarakat umum, yang artinya bersifat bebas di gunakan oleh semua kalangan, namun tetap mematuhi aturan yang berlaku.

Semua jaringan wifi mempunyai cakupan area yang berbeda-beda, tergantung daya dan jenis antenna yang digunakan. Tidak mudah untuk menghalang jaringan wi-fi jika lokasi tersebut masuk kedalam cakupan area tersebut [2].

Peluang terjadinya sinyal jamming sangat dimungkinkan. baik secara di sadari maupun tidak karena ketidakpahaman pengguna pada sistem keamanan dan cara kerja jaringan tersebut. Sistematis penggunaan kanal frekuensi adalah kewajiban supaya sinyal jamming mampu di minimalisir. Jamming terjadi lantaran frekuensi yang pakai lumayan sempit maka penggunaan kembali channel cukup sulit dilakukan pada cakupan yang terdapat banyak jaringan wireless.

Wemos d1 mini merupakan sebuah modul WiFi berbasis ESP-8266. Pada Wemos d1 mini memiliki chip on board, sehingga tidak memerlukan kembali mikrokontroler sebagai pengolah informasi. Wemos d1 mini juga mempunyai pin digital dan pin analog yang berfungsi menghubungkan sensor ataupun actuator. Wemos d1 mini dapat diprogram menggunakan IDE Arduino [4]

Tulisan ini dibagi menjadi empat bagian, yaitu pendahuluan yang memberikan gambaran latar belakang pengembangan sistem dan penelitian terkait. Bagian kedua adalah metode yang digunakan untuk membangun simulasi serangan, Selanjutnya adalah bagian hasil dan pembahasan yang memaparkan hasil dan uji coba simulasi. Tulisan ditutup dengan kesimpulan hasil penelitian.

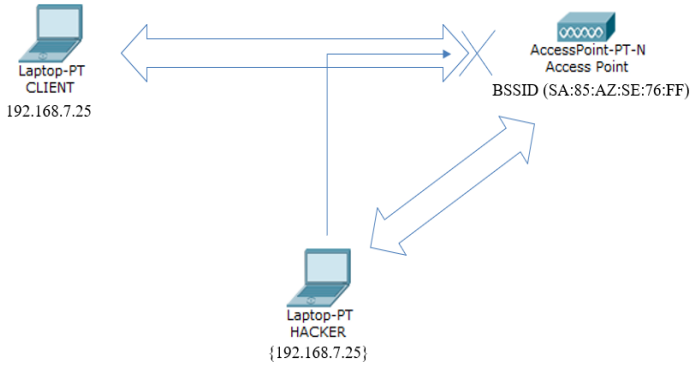
2. METODE

Pada penelitian ini, metode yang digunakan adalah simulasi jamming terhadap keamanan jaringan nirkabel akses point WPA2/AES untuk mengetahui kelemahan teknologi tersebut. Setelah itu, hasil ditabulasi dan dianalisa. Wemos D1 Mini merupakan perangkat yang dipergunakan untuk melakukan jamming pada sebuah sistem jaringan tanpa kabel.

Simulasi serangan jamming yang dilakukan dibagi menjadi **dua *serangan***, yaitu :

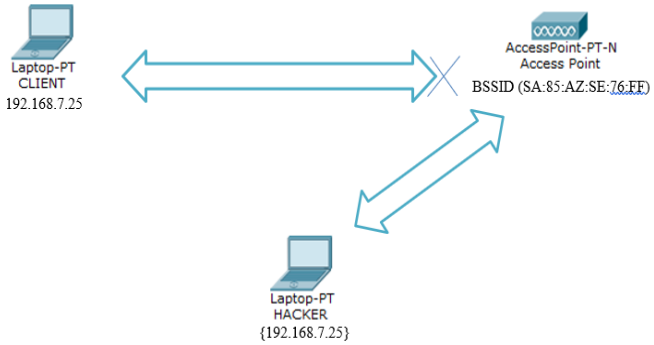
1) Session hijacking merupakan salah satu serangan efektif pada jaringan, cukup mudah dan apabila jalur akses target tidak menggunakan enkripsi WEP/WPA. Dengan melakukan session hijacking, seorang penyerang dapat memperoleh akses ke suatu jaringan, dimana penyerang menyamar sebagai pengguna yang sah. Metode

ini juga dapat menjadi langkah pertama dalam berbagai teknik serangan yang lebih rumit (Herdiana, 2014)



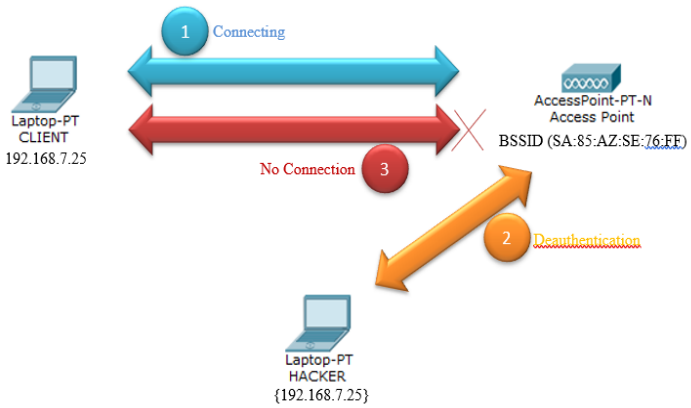
Gambar 1. Skema Serangan Session hijacking

2) Serangan Deauth merupakan serangan yang berfungsi untuk mematikan fungsi accesss point target, caranya dengan mengklik menu start dan tunggu beberapa saat, maka fungsi accesss point (AP) akan mati dan Klien yang terhubung dengan AP tersebut otomatis akan terputus.



Gambar 2. Skema Serangan Deauth

Mekanisme serangan :



Gambar 3. Skema Serangan Sinyal Jamming

Simulasi yang dilakukan pada percobaan ini sebanyak 15 kali yang terbagi pada 3 skenario, berikut :

a. Skenario Pertama

Serangan dilakukan pada jarak 5 meter dari akses point dengan variasi perangkat yang terhubung ke akses point yaitu, satu perangkat, dua perangkat, tiga perangkat, empat perangkat dan lima perangkat.

b. Skenario Kedua

Serangan dilakukan pada jarak 15 meter dari akses point dengan variasi perangkat yang terhubung ke akses point yaitu, satu perangkat, dua perangkat, tiga perangkat, empat perangkat dan lima perangkat.

c. Skenario Ketiga

Serangan dilakukan pada jarak 25 meter dari akses point dengan variasi perangkat yang terhubung ke akses point yaitu, satu perangkat, dua perangkat, tiga perangkat, empat perangkat dan lima perangkat.

Adapun alat dan bahan yang digunakan adalah :

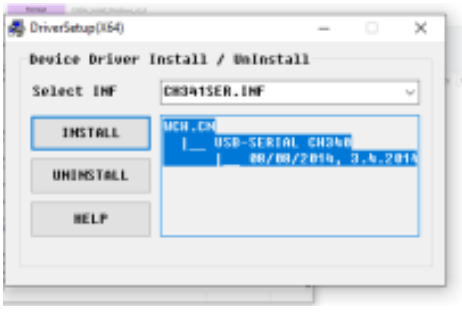
Tabel Alat dan bahan.

Alat	Bahan
PC/Laptop	Driver windows (64bit)
Telepon genggam	Software deauther 2.1.0_1MB.bin
AP	Software ESP8266Flasher 64bit
Wemos d1 mini	Web browser
Kabel USB	

Langkah-langkah yang diperlukan untuk melakukan sinyal jamming untuk mengkonfigurasi wemos D1 mini serta menghubungkan dengan perangkat PC/Laptop penyerang, sebagai berikut :

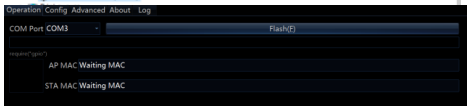
a. Mengatur wemos d1 mini

b. Mengunduh device driver untuk sistem operasi windows 10



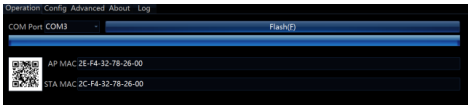
c. Mengecek device manager, dan membuka bagian ports kemudian pastikan ada USB-Serial

d. Membuka software ESP8266 Flasher 64.exe



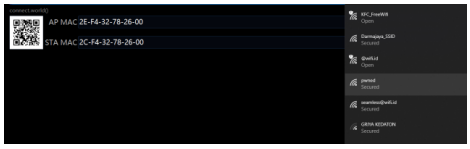
e. Membuka menu config dan klik INTERNAL ://NODEMCU kemudian pilih deauther bin

f. Membuka menu operation dan klik “Flash”, tunggu beberapa saat hingga proses tersebut selesai

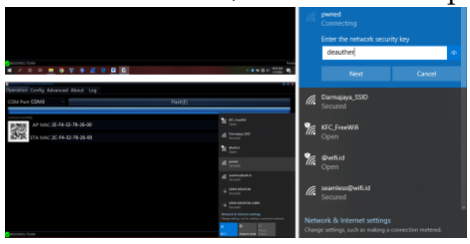


g. Setelah proses selesai, kemudian maka akan terbuat Accesss point baru dengan MAC 2E-F4-32-78-26-00

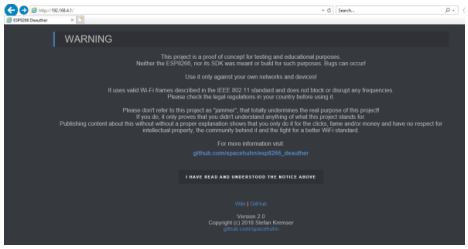
h. Kemudian akan muncul SSID wemos d1 mini yaitu pwned



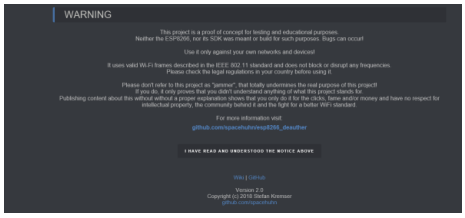
i. Kemudian masuk, dan masukkan password “deauther”.



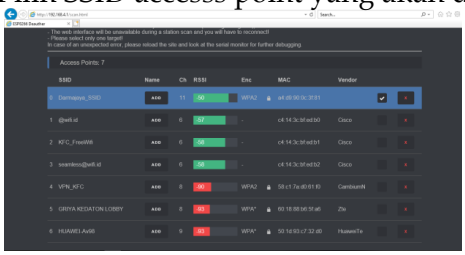
j. Gunakan smartphone/laptop untuk melakukan serangan



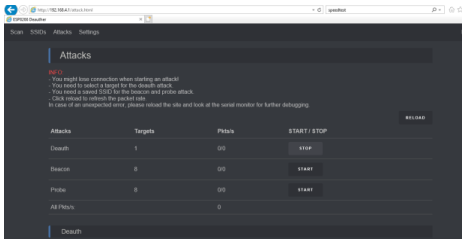
k. Klik menu " I HAVE READ AND UNDERSTOOD THE NOTICE ABOVE "



l. Pilih SSID accesss point yang akan diserang



m. Klik menu ATTACKS, dan mulai penyerangan terhadap accesss point



Percobaan ini telah di lakukan secara berkesinambungan dengan perangkat yang sama namun dengan kombinasi perangkat terkoneksi yang berbeda-beda pada jarak 5 meter, 15 meter dan 25 meter. Berikut tabulasi simulasi atau percobaan yang dilakukan:

Tabel 1. Tabulasi simulasi atau percobaan

No. Percobaan	Jarak	Perangkat Terkoneksi		Kecepatan/Kekuatan Sinyal			Durasi Accesss Point Down
		Jumlah Perangkat	Jenis Perangkat	Download mbps	Unggahan mbps	Latensi	
1	5 Meter	1	Xiaomi MiA2 Lite	1.38	1.81	16 md	00:00:10.06
2		2	Asus X441B	1.59	1.65	16 md	00:00:34.99
			Xiaomi MiA2 Lite	1.64	1.76	15 md	00:00:11.09
3		3	Xiaomi Redmi 4X	6.81	2.25	16 md	00:00:05.23
			Asus X441B	0.25	1.74	16 md	00:00:07.44
			Xiaomi MiA2 Lite	6.81	0.19	16 md	00:00:04.14
4		4	Xiaomi Redmi 5	4.05	1.42	16 md	00:00:04.41
			Xiaomi Redmi 4X	1.38	0.54	85 md	00:00:04.11
			Asus X441B	2.59	1.21	62 md	00:01:33.63
			Xiaomi MiA2 Lite	0.81	0.69	67 md	00:02:34.10
5		5	Acer Aspire 5	1.51	1.76	76 md	00:00:53.73
			Xiaomi Redmi 5	2.44	6.10	16 md	00:00:06.60
			Xiaomi Redmi 4X	5.03	2.09	16 md	00:00:04.49
			Asus X441B	6.28	1.80	16 md	00:01:37.32
			Xiaomi MiA2 Lite	0.66	0.11	427 md	00:02:40.57
6	15	1	Xiaomi MiA2 Lite	5.30	1.79	17 md	00:00:05.95

7	Meter	2	Xiaomi MiA2 Lite	3.81	0.46	17 md	00:00:04.75
			Asus X441B	0.93	1.32	324 md	00:00:35.31
8		3	Xiaomi MiA2 Lite	2.90	0.52	84 md	00:00:05.23
			Asus X441B	3.42	1.64	16 md	00:00:28.66
			Xiaomi Redmi 5	4.58	0.53	17 md	00:00:03.51
9		4	Xiaomi MiA2 Lite	2.83	0.35	17 md	00:02:55.80
			Asus X441B	0.09	1.42	486 md	00:00:48.04
			Xiaomi Redmi 5	1.74	0.53	17 md	00:00:06.12
			Acer Aspire 5	2.67	1.47	17 md	00:00:17.64
10		5	Xiaomi MiA2 Lite	3.03	1.95	17 md	00:00:09.69
			Asus X441B	0.19	1.81	197 md	00:00:22.06
			Xiaomi Redmi 4X	0.51	0.79	17 md	00:00:09.06
			Xiaomi Redmi 5	2.02	2.07	17 md	00:00:20.24
			Acer Aspire 5	0.86	0.54	132 md	00:00:13.26
11	25 Meter	1	Acer Aspire 5	7.38	1.90	18 md	00:00:09.65
12		2	Xiaomi Redmi 5	0.55	1.65	18 md	00:00:06.54
			Acer Aspire 5	1.85	1.61	18 md	00:00:10.66
13		3	Xiaomi Redmi 5	0.30	2.02	18 md	00:00:03.38
			Xiaomi MiA2 Lite	1.50	0.28	122 md	00:00:06.15
			Acer Aspire 5	0.29	1.48	18 md	00:00:07.13
14		4	Xiaomi Redmi 5	0.30	1.34	18 md	00:00:03.95
			Xiaomi Redmi 4X	0.05	0.88	259 md	00:00:02.33
			Xiaomi MiA2 Lite	0.30	0.31	18 md	00:00:03.04
			Acer Aspire 5	0.29	1.67	18 md	00:00:05.79
15		5	Xiaomi MiA2 Lite	1.49	0.74	18 md	00:00:03.71
			Asus X441B	0.27	0.37	19 md	00:00:15.55
			Xiaomi Redmi 4X	0.49	0.44	16 md	00:00:11.35
			Xiaomi Redmi 5	5.52	1.69	18 md	00:00:04.22
			Acer Aspire 5	4.32	1.72	18 md	00:00:05.88

3. HASIL DAN PEMBAHASAN

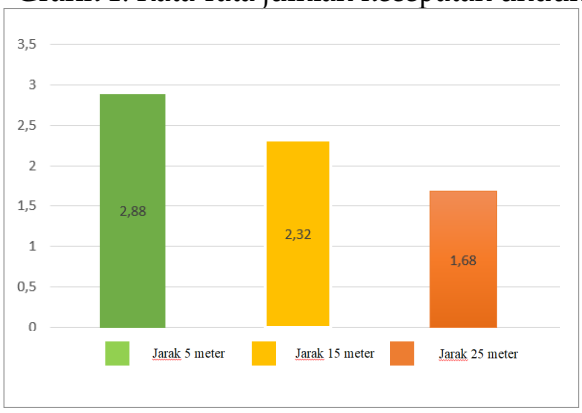
WPA menggunakkan teknologi atau algoritma untuk autentikasi pengguna, tetapi teknologi tersebut tidak bisa melindungi sistem dari serangan sinyal jamming.

Pada penelitian ini, semua percobaan berhasil meluncurkan serangan jamming AP dengan variasi jarak percobaan, kecepatan/kekuatan signal (unduh, unggahan, latensi), dan durasi jamming yang berbeda-beda seperti pada (tabel 1).

a. Kecepatan/Kekuatan Sinyal (unduh)

Berdasarkan penelitian yang telah dilakukan, maka didapat rata-rata jumlah kecepatan download sebagai berikut.

Grafik 1. Rata-rata jumlah kecepatan unduh



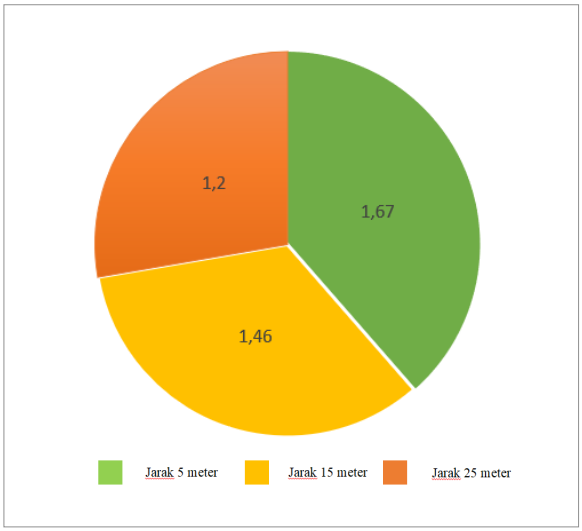
Kecepatan/kekuatan sinyal (unduh) sangat mempengaruhi proses penyerangan yang dilakukan. Apabila kecepatan/kekuatan sinyal (unduh) perangkat penyerang berada pada jarak yang dekat dengan AP, maka akan lebih mudah dan lebih cepat untuk melakukan jamming. Terlihat pada percobaan 1 yang memiliki kecepatan/kekuatan sinyal (unduh) 1,38 mbps pada jarak 5 meter dari AP, apabila dibandingkan dengan percobaan 7 yang memiliki 0,93 mbps pada jarak 15 meter dari AP. Maka dapat dibuktikan bahwa percobaan 1 lebih mudah dan lebih cepat untuk melakukan jamming AP lemah/*down* yaitu selama 10,06 detik. Seperti halnya pada percobaan 3 yang memiliki kecepatan/kekuatan sinyal (unduh) 6,81 mbps pada jarak 5 meter dari AP, apabila dibandingkan dengan percobaan 9 yaitu 2,83 mbps pada jarak 25 meter dari AP. Hal ini berarti, percobaan 3 lebih mudah dan lebih cepat untuk melakukan serangan hingga AP mengalami denial of service (DoS) diperlukan 5,23 detik.

Sedangkan, apabila kecepatan/kekuatan sinyal (unduh) perangkat penyerang berada pada jarak yang jauh dari AP, maka akan lebih sulit dan lebih lama untuk melakukan jamming. Hal ini terjadi karena pada proses jamming dimulai secara terstruktur yaitu dimulai dari area terdekat hingga ke area berikutnya. Terlihat pada percobaan 8 yang memiliki kecepatan/kekuatan sinyal (unduh) 4,58 mbps pada jarak 15 meter dari AP, apabila dibandingkan dengan percobaan 15 dengan kecepatan/kekuatan sinyal (unduh) 0,27 mbps pada jarak 25 meter dari AP. Hal ini membuktikan bahwa percobaan 15 lebih sulit dan lebih lama untuk melakukan jamming hingga AP tidak dapat melakukan layanan lagi diperlukan waktu 15,55 detik. Seperti halnya pada percobaan 4 yang memiliki kecepatan/kekuatan sinyal (unduh) 4,05 mbps pada jarak 5 meter dari accesss point, apabila dibandingkan dengan percobaan 12 yaitu 1,85 mbps pada jarak 25 meter dari AP, maka dapat dibuktikan bahwa percobaan 12 lebih sulit dan lebih lama untuk melakukan jamming dengan durasi serangan adalah 10,66 detik.

b. Kecepatan/Kekuatan Sinyal (Unggahan)

Berdasarkan percobaan yang telah dilakukan, maka didapat rata-rata jumlah kecepatan unggahan sebagai berikut :

Grafik 2. Rata-rata jumlah kecepatan unggahan



Simulasi pada jarak 5 meter memiliki rata-rata kecepatan unggahan sebesar 1,2 mbps, pada jarak 15 meter 1,46 mbps dan pada jarak 25 meter sebesar 1,67 mbps. Hal ini menandakan bahwa kecepatan/kekuatan sinyal (unggahan) sangat mempengaruhi proses jamming yang dilakukan. Apabila perangkat penyerang berada pada jarak yang dekat dengan AP, maka akan lebih mudah dan lebih cepat untuk melakukan jamming. Dapat

dibuktikan pada percobaan 4 yang memiliki kecepatan/kekuatan sinyal (unggahan) 0,54 mbps pada jarak 5 meter dari AP, jika dibandingkan dengan percobaan 8 dengan 1,64 mbps pada jarak 15 meter dari AP. Hal ini menunjukan bahwa percobaan 8 lebih sulit dan lebih lama untuk melakukan jamming hingga accesss point mengalami pelemahan diperlukan waktu 28,66 detik.

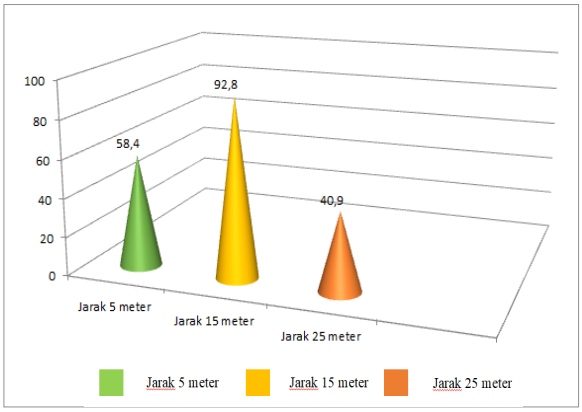
Apabila perangkat penyerang berada pada jarak yang jauh dari AP, maka akan lebih sulit dan lebih lama untuk melakukan jamming. Percobaan 5 yang memiliki kecepatan/kekuatan sinyal (unggahan) 6,10 mbps pada jarak 5 meter dari accesss point, apabila dibandingkan dengan percobaan 9 yang memiliki 0,35 mbps pada jarak 15 meter dari AP. Terbukti, bahwa percobaan 9 lebih sulit dan lebih lama untuk melakukan jamming hingga AP *down* yaitu berdurasi 2 menit 55,80 detik.

c. Kecepatan/Kekuatan Sinyal (Latensi)

Latensi adalah jeda waktu yang dibutuhkan dalam pengantaran data dari pengirim ke penerima. Makin tinggi jeda waktu maka makin lambat penerima merespons perintah dari pengirim

Berdasarkan simulasi yang telah dilakukan, maka didapat rata-rata latensi sebagai berikut.

Grafik 3. Rata-rata latensi percobaan



Rata-rata latensi percobaan pada jarak 5 meter sebesar 58.4 milidetik, pada jarak 15 meter 92.8 milidetik dan pada jarak 25 meter sebesar 40.9 milidetik. Hal ini membuktikan bahwa latensi pada percobaan ini tidak berpengaruh pada saat jamming diluncurkan.

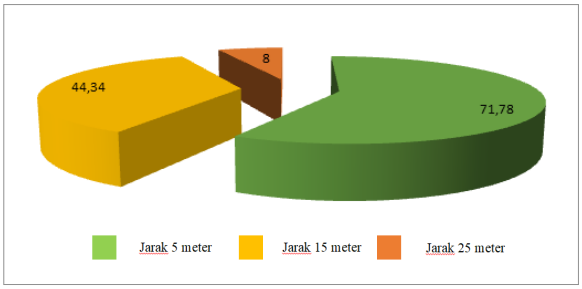
Jarak maupun waktu accesss point down tidak dipengaruhi oleh latensi. Dapat dibuktikan pada percobaan 9 yang memiliki latensi 486 milidetik pada jarak 15 meter dari accesss point, dengan durasi jamming 48,04 detik. Pada percobaan 14 yang memiliki latensi 259 milidetik pada jarak 25 meter dari accesss point, dengan durasi jamming 2,33 detik.

Apabila dibandingkan dengan percobaan 4 yang memiliki latensi 85 milidetik pada jarak 5 meter dari accesss point, dengan durasi jamming 4,11 detik. Pada percobaan 6 yang memiliki latensi 17 milidetik pada jarak 15 meter dari accesss point, dengan durasi jamming 5,95 detik.

d. Durasi Accesss Point Down

Berdasarkan simulasi yang telah dilakukan, maka didapat rata-rata lamanya accesss point mengalami denial of service sebagai berikut :

Grafik 4. Durasi Accesss Point Down



Rata-rata durasi AP mengalami pelemahan yaitu percobaan pada jarak 5 meter yaitu 00:01:11.78 detik, pada jarak 15 meter 00:00:44.34 detik dan pada jarak 25 meter sebesar 00:00:08.00 detik. Hal ini membuktikan bahwa semakin dekat jarak maka durasi yang AP mengalami denial of service semakin lama.

4. KESIMPULAN

Keamanan pada jaringan wireless LAN sangat penting khususnya untuk menjamin agar pihak yang mengakses jaringan adalah yang sah. Untuk itu, WPA2 menggunakan sistem keamanan yang cukup baik, yakni AES (Advanced Encryption Standar) meskipun demikian, jaringan wireless LAN memiliki celah kelemahan terhadap serangan salah satunya menggunakan serangan sinyal jamming dengan menggunakan alat wemos d1 mini.

Untuk mengetahui ketahanan sistem keamanan pada jaringan nirkabel terhadap kejahatan serangan sinyal jamming, uji coba yang dilakukan dengan kombinasi jarak, jumlah perangkat dan jenis perangkat menggunakan Wemos d1 mini.

Berdasarkan uji coba yang telah dilakukan, bahwa jarak dan kekuatan sinyal sangat berpengaruh pada proses jamming yang dilakukan. Kecepatan/kekuatan sinyal (unduh) dan kecepatan/kekuatan sinyal (unggahan) mempengaruhi durasi access point down.

Dapat di simpulkan bahwa semakin dekat jarak penyerang pada accesss point maka akan semakin lama durasi accesss point down. Namun sebaliknya, semakin jauh jarak penyerang pada accesss point maka akan semakin cepat durasi accesss point down.

DAFTAR RUJUKAN

[1] Agustiningsih, R., Suryadi, D., & D. (2018). No Title. *Rancang Bangun Alat Pemblocking Sinyal (Jammer) Pada Sistem Telekomunikasi Jaringan Seluler Global System For Mobile (GSM) Di Area Bebas Sinyal GSM.*, 946–952. http://jurnal.untan.ac.id/index.php/jteuntan/article/view/25220

[2] Herdiana, Y. (2014). No Title. *Keamanan Pada Jaringan Wireless*, *7(2)*(Isu Teknologi STT Mandala), 25–36.

[3] Jamaludin. (2016). No Title. *Teknik Keamanan Jaringan Wireless LAN Pada Warnet Salsabila Computer Net. Jurnal & Penelitian Teknik Informatika*, *1*, 67–74.

[4] Khalif, M. I., Syauqy, D., & Maulana, R. (2018). No Title. *Pengembangan Sistem Penghitung Langkah Kaki Hemat Daya Berbasis Wemos D1 Mini*, *2(6)*, 2211–2220.

[5] Septiawan, R., Astawa, I. M., Rufiyanto, A., Agastani, T., & Rahmatullah, R. (2019). No Title. *Metode Deteksi ' Potential Security Threats ' Pada ADS-B Data Dengan Memonitor EM Emisi Radiasi Pada Jaringan Ethernet*, *XI(1)*.