Implementasi Serangan *Ip Spoofing*Dan *Relay Attack* Pada *Software Defined Network* (Sdn)

1st Myra Tresno Karimah
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
myraakarimah@telkomuniversity.ac.id

2nd Mochamad Teguh Kurniawan
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
teguhkurniawan@telkomuniversity.ac.id

3rd Adityas Widjajarto
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
adtwjrt@telkomuniversity.ac.id

Abstrak **- Software-Defined Networking rentan terhadap serangan karena sifatnya yang terbuka dan dapat diprogram. Penelitian penting untuk meningkatkan keamanannya. IP Spoofing adalah pemalsuan alamat IP untuk mengelabui sistem keamanan. Relay Inject Attack menyisipkan tautan palsu antara dua switch dalam pandangan pengontrol. Penelitian ini membahas implementasi serangan dan analisis latency Relay Attack & IP Spoofing pada SDN. Pengujian Relay Attack akan dilakukan dengan scapy script, & IP Spoofing dengan IP decoy Nmap dengan membanjiri SYN Packet. Analisa meliputi latency, perubahan aliran jaringan pada Flow Table, dan intersepsi terhadap link palsu yang memanipulasi trafik jaringan.**

Kata Kunci**- Relay Attack, IP Spoofing, Software Defined Network, Kerentanan SDN**

I. PENDAHULUAN

Pengenalan Software-Defined Networking (SDN) sebagai paradigma baru dalam jaringan komputer telah menarik perhatian industri dan akademisi. SDN memungkinkan pengelolaan jaringan yang terpusat, memungkinkan konfigurasi yang seragam bahkan dengan perangkat dari vendor yang berbeda. Namun, sifat terbuka dan dapat diprogramnya SDN menjadikannya rentan terhadap serangan, memerlukan penelitian untuk meningkatkan keamanannya.

Serangan seperti IP Spoofing dan Relay Inject Attack dapat terjadi dalam konteks SDN. IP Spoofing membingungkan deteksi serangan karena serangan tersebut tampak berasal dari alamat IP yang sah. Sementara Relay Inject Attack menyisipkan tautan palsu di antara dua sakelar yang sah dalam pandangan pengontrol.

Penelitian ini bertujuan untuk memahami mekanisme dan dampak dari serangan Relay Attack dan IP Spoofing pada SDN melalui serangkaian skenario pengujian yang mencakup berbagai aspek, termasuk analisis paket dengan alamat IP palsu dan intersepsi fake link yang memanipulasi lalu lintas jaringan. [1]

Penelitian ini mengimplementasikan serangan-serangan tersebut dan menganalisis dampaknya terhadap latensi di jaringan SDN. Pengujian dilakukan melalui skrip Scapy untuk Relay Attack, dan dengan Nmap menggunakan IP umpan untuk IP Spoofing dengan SYN Packet flooding. Analisis meliputi evaluasi latensi, perubahan aliran jaringan di Flow Table, serta intersepsi link palsu yang memanipulasitrafik jaringan.

II. KAJIAN TEORI

Dalam konteks kajian teori ini, kajian teori ini menguraikan beberapa kerentanan yang terkait dengan keberadaan SDN, seperti kurangnya kontrol terhadap aplikasi pihak ketiga, ketergantungan terhadap protokol OpenFlow, dan potensi ancaman yang mungkin muncul dari serangan IP Spoofing dan Relay Attack. Selanjutnya akan dijelaskan implementasi serangan dan dampak dari analisis latency dalam konteks serangan Relay Attack dan IP Spoofing pada SDN..

A. Kerentanan SDN

Kerentanan dalam Software Defined Network (SDN) muncul karena pemisahan antara bidang kontrol dan bidang data.[4] Kerentanan ini termasuk tidak adanya manajemen jaringan yang terpusat, kurangnya mekanisme untuk mencegah alokasi data atau paket yang salah pada lapisan data, kontrol yang terbatas terhadap aplikasi pihak ketiga dan sistem operasi (OS), ketergantungan jaringan pada protokol OpenFlow, kontrol yang tidak memadai terhadap API yang tidak aman, dan ketidakmampuan untuk melindungi dari kesalahan konfigurasi. [1] Kerentanan ini dapat mengakibatkan ancaman seperti penggunaan pengontrol yang tidak sah, penggunaan aplikasi yang tidak sah, kebocoran data, kompromi data akun, modifikasi data, aplikasi berbahaya, ancaman terhadap sistem operasi, tidak adanya TLS, ancaman terhadap elemen protokol, penyalahgunaan OpenFlow, API yang rentan, risiko manusia, dan ancaman kesalahan konfigurasi.

B. *Relay Attac*k

Dalam Relay Attack, penyerang meneruskan frame LLDP asli untuk membuat koneksi palsu di SDN [3]. Serangan ini

memiliki dua dampak utama: meningkatkan penundaan transmisi frame LLDP yang sesuai, dan membuat alamat IP host korban muncul lebih sering dalam rentang tertentu, menyebabkan kebingungan dan gangguan.[5] Penjelasan ini menyoroti bagaimana penyerang memanipulasi pembuatan frame LLDP melalui pemalsuan dan Relay Attack, yang berpotensi membuat koneksi palsu di SDN dan mengganggu komunikasi dan keamanan jaringan.

C. *IP Spoofing*

IP Spoofing adalah teknik penting yang digunakan oleh penyerang untuk menyembunyikan identitas asli mereka dan menghindari pelacakan sumber serangan [4]. Dengan mengubah alamat IP sumber dalam sebuah serangan, penyerang membuat serangan tersebut tampak berasal dari sumber yang sah, sehingga menghindari deteksi dan tindakan respons.

D. *QoS Testing*

Quality of Service (QoS) adalah seperangkat teknik yang mengatur kinerja jaringan, termasuk bandwidth, delay (latensi), jitter, dan packet loss, untuk menyediakan layanan yang andal dan berkualitas bagi pengguna akhir. QoS berfokus pada peningkatan produktivitas pengguna dan menyediakan layanan yang dapat diandalkan untuk aplikasi berbasis jaringan [5].

E. Latency(Delay)

Pada penelitian ini, parameter QoS utama yang menjadi fokus adalah Latency (Delay), yaitu waktu yang dibutuhkan data untuk melakukan perjalanan dari sumber ke tujuan. Penelitian ini mengacu pada standar TIPHON (*Telecommunications and Internet Protocol Harmonization Over Networks*) untuk mengukur dan memonitoring kinerja jaringan komunikasi [5]. Tujuannya adalah untuk mengoptimalkan jaringan agar aplikasi berbasis jaringan dapat berjalan lebih baik bagi pengguna akhir.

Kategory Delay	**Besar Delay**	**Indeks**
Sangat Bagus	<150 ms	4
Bagus	150 ms-300 ms	3
Sedang	300 ms-450 ms	2
Tidak Bagus	>450ms	1

TABEL 1, STANDAR TIPHON DALAM PENGUKURAN LATENCY(DELAY)

(A)

$$Rata\ rata\ Delay = \frac{\text{Jumlah Delay}}{\text{Jumlah Packet Yang Diterima}}$$

Untuk memastikan pengukuran rata-rata latency dari data hasil analisis agar dapat dikategorikan dalam standar TIPHON, maka perlu digunakan rumus rata-rata, meskipun pada penelitian ini, penulis mencatat rata-rata secara langsung dari output analisis RTT dengan perintah ping.

III. METODE

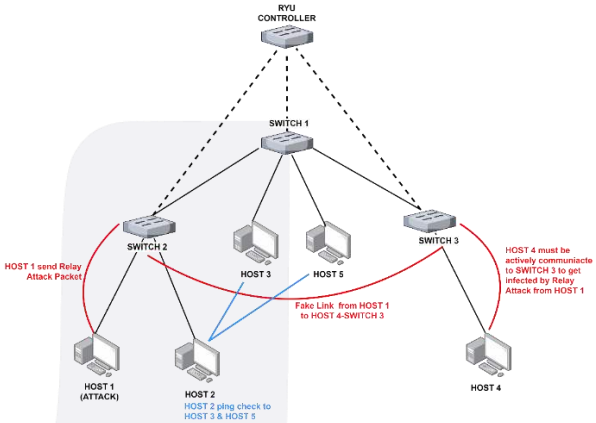
Dalam penelitian ini, desain sistem dan skenario serangan mengikuti kerangka kerja PPDIOO (Prepare-Plan-Design-Implement-Operate-Optimize), yang mana pada penelitian ini dibatasi hingga tahap Desain.:

A. Prepare

Dalam mekanisme serangan Relay Attack dengan fake link, attacker (Host 1) menggunakan port terinfeksi di switch untuk mengalihkan paket ke switch lain, menciptakan fake link antara dua switch yang sebenarnya tidak terhubung. Dengan memanipulasi paket kontrol LLDP, attacker memasukkan informasi palsu tentang fake link ini, mengganggu aliran lalu lintas jaringan. Setelah fake link terbentuk, attacker dapat melakukan serangan seperti IP spoofing. Dengan IP spoofing, attacker memalsukan alamat IP sumber pada paket yang dikirim melalui fake link tersebut, menyembunyikan identitasnya dan mengarahkan lalu lintas paket ke target yang tidak semestinya.

B. Plan & Design

Pada subbab ini, kami akan membahas dua teknik serangan yang signifikan dalam konteks jaringan, yaitu Relay Attack dan IP Spoofing. Relay Attack memungkinkan pembuatan Fake Link dengan cara menyadap dan meneruskan paket melalui host yang terhubung ke switch lain. Di sisi lain, IP Spoofing melibatkan manipulasi alamat IP pengirim paket untuk mengelabui penerima dengan menyembunyikan sumber sebenarnya.



GAMBAR 1,
TOPOLOGI JARINGAN(A)

Dalam eksperimen yang akan di jelaskan, terdapat penggunaan Relay Attack yang digunakan untuk menciptakan Fake Link antara dua switch yang seharusnya tidak terhubung, mengizinkan pengiriman ulang paket kontrol LLDP dan menghasilkan duplikasi paket saat berkomunikasi. Selanjutnya, kami akan melihat bagaimana serangan IP Spoofing dieksekusi setelah berhasil membentuk Fake Link, dengan penyerang (host1) mengatasnamakan alamat IP host 2(10.1.1.2) untuk mengaburkan jejaknya. Mari kita eksplorasi lebih lanjut teknik-teknik ini dan dampaknya pada kualitas jaringan.

Skenario	**Detail**	**Tujuan**
Relay Attack	Relay Attack dapat membuat *Fake Link* dengan menyadap dan meneruskan paket yang masuk dari port yang disusupi pada satu host	switch S2 dan S3 tidak terhubung secara langsung. Host 1 sebagai penyerang mengeksekusi script sniff untuk mendapatkan akses

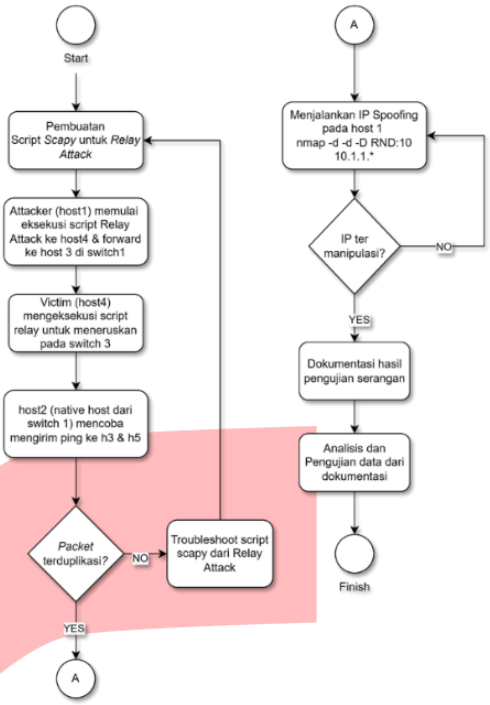
Skenario	Detail	Tujuan
	yang terhubung pada switch ke switch lain.	ke kedua switch dan bertindak sebagai Relay Attacker. Hal ini memungkinkan untuk membuat fake link dengan merelay paket kontrol LLDP, sehingga terjadi duplikasi packet saatberkomunikasi
IP Spoofing	IP spoofing melibatkan manipulasi alamat IP pengirim paket untuk membuatnya terlihat berasal dari sumber yang berbeda.	Penyerangan dilakukan setelah berhasil membentuk fake link antara S2 dan S3, attacker (host1) kemudian melanjutkan serangan dengan teknik IP spoofing mengatasnamakan IP host 2(10.1.1.2)

TABEL 1,
Tabel Skenario Dan Tujuan Masing Masing Serangan
(A)

Rancang serangan menggambarkan langkah-langkah utama dalam eksperimen. Pertama, attacker (host1) menggunakan script relay attack melalui Scapy untuk mengirim paket yang dimanipulasi melalui host4 ke host3. Kemudian, victim (host4) meneruskan paket tersebut ke switch3 sebagai perantara. Host 2 mengirim ping ke host3 dan host5 untuk memeriksa duplikasi paketakibat relay attack.

Langkah kedua melibatkan IP spoofing oleh attacker utama (host1) menggunakan nmap dengan alamat IP palsu yang mengaburkan asal paket. Hasil IP spoofing diperiksa dan didokumentasikan untuk analisis selanjutnya terkait dampak dan kerentanan serangan.

Dalam keseluruhan perancangan ini, dari relay attack hingga IP spoofing, langkah-langkah ini membentuk sistem yang terperinci untuk menjalankan eksperimen, menganalisis hasilnya, dan memahami dampak serta potensikerentanan serangan pada jaringan SDN.



GAMBAR 1 perancangan sustem
(A)

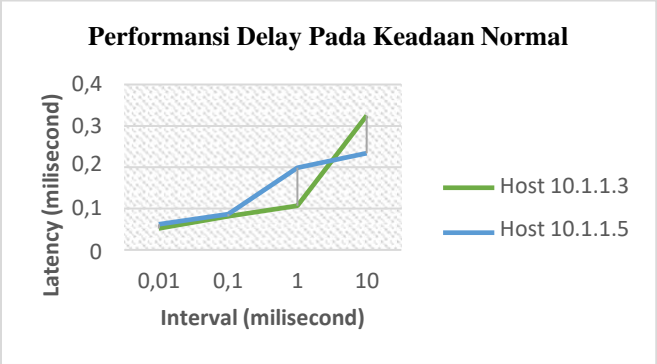
IV. HASIL DAN PEMBAHASAN

F. Hasil Pengujian Serangan

Dalam subbab ini, kami akan mendalami analisis Testing Period ping untuk memahami dampak serangan lebih mendalam. Untuk mencapai pemahaman yang lebih detail dan terperinci, kami membagi Testing Period analisis menjadi 0.010 milisecond, 0.10 milisecond, 1 milisecond, dan 10 milisecond. Dengan demikian, kami dapat memetakan perubahan latensi dengan jelas dalam Testing Period yang telah ditentukan.

Penulis akan menggambarkan analisis ini dengan menggunakan command ping yang dilakukan dari host2 untuk menguji dampak serangan pada host3 dan host5. Dengan total 100 ping, kami akan mengamati bagaimana variasi Testing Period ping ini memengaruhi respons jaringan dan membantu kami mengidentifikasi dampak serangan dengan lebih akurat. Berikut hasil analisis ini dalam subbab ini.

Latency normal rata rata (avg.)				
Testing Period	**Host 10.1.1.3**	**Durasi**	**Host 10.1.1.5**	**Durasi**
0.010ms	0.052ms	1604 ms	0.062ms	1747 ms
0.100ms	0.081ms	10551 ms	0.087ms	11662 ms
1 ms	0.107ms	101907 ms	0.199ms	101441 ms
10 ms	0.325ms	1009113 ms	0.234ms	1011293 ms



Terpapar pada Tabel 5.3.2 Dan Gambar 5.3.1 bahwa rata rata seluruh latency pada Host 10.1.1.3 dan Host 10.1.1.5 sebelum adanya serangan berada di bawah 1 millisecond, dengan durasi antar Testing Period yang menyesuaikan dengan jarakpada host 10.1.1.2 sebagai penguji analisis dengan ping.

G. Analisis Data Serangan Pada 10.1.1.3 (Host 5)

Pada analisis data serangan pada Host 3 (10.1.1.3), Parameter delay diuji berdasarkan hasil pengamatan menggunakan command ping

Menurut analisa data pada tabel Setelah terjadinya Relay Attack (Fake link), terjadi lonjakan pada delay(latency) yang terpapar pada tabel tersebut serta ditujukan adanya rata rata delay terendah ada pada pengujian dengan Testing Period 0.010 millisecond dengan latency 575,613 millisecond, serta adanya rata rata tertinggi ada pada pengujian dengan Testing Period 10 millisecond dengan latency 308061,564 millisecond.

Selanjutnya, dilakukan pendataan Latency(Delay) dari host2 ke host 3 pada serangan Flood IP Spoof, berikut terlampir tabel data hasil dari analisa latensi menggunakan ping:

Ip spoof Host 10.1.1.3			
Testing Period (ms)	**Latency (ms)**	**Durasi**	**Duplikasi**
0.010ms	**119.095 ms**	1528 ms	20
0.100ms	**1347.642 ms**	10194 ms	129
1 ms	**22707.677 ms**	99210 ms	2027
10 ms	**260603.086 ms**	100590 ms	23756

Hasil pengujian latency(delay) dari serangan IP Spoofing pada host3yang terpapar pada tabel 5.3.5 Setelah terjadinya IP Spoof, terjadi lonjakan pada delay(latency) yang terpapar pada tabel tersebut serta ditujukan adanya rata rata delay terendah ada pada pengujian dengan Testing Period 0.010 millisecond dengan latency 119,095 millisecond, serta adanya rata rata tertinggi ada pada pengujian dengan Testing Period 10 millisecond dengan latency 260603,086 millisecond.

Indexing Parameter QoS Delay (Relay Attack) standar TIPHON					
Testing Period (ms)	**Min (ms)**	**Max (ms)**	**Rata-rata (ms)**	**Indeks**	**Kategori**
0.010ms	0,013	1657,41	**575,613**	1	Tidak Bagus
0.100ms	0,020	2103,949	**1106,791**	1	Tidak Bagus
1 ms	0,022	95453,255	**25586,219**	1	Tidak Bagus
10 ms	0,025	986236,197	**308061,564**	1	Tidak Bagus
Rata-rata	0.020	270948,357	**83832,547**	1	Tidak Bagus

Berdasarkan data pengujian Relay Attack pada host3 dari tabel diatas, latency (delay) memiliki nilai minimal pada Testing Period 0.010 millisecond (575,613 ms) dan nilai maksimal pada Testing Period 10 millisecond (83,832,547 ms). Ini mengindikasikan bahwa selama serangan Relay Attack, kualitas komunikasi jaringan pada host3 dapat dikategorikan sebagai "Tidak Bagus" berdasarkan standar TIPHON dengan nilai Index 1, karena rata-rata delay packet data melebihi 450 ms.

Relay Attack Host 10.1.1.3			
Testing Period (ms)	**Host 10.1.1.3 (ms)**	**Durasi**	**Duplikasi**
0.010ms	**575.613 ms**	10043 ms	79
0.100ms	**1106.791 ms**	10220 ms	180
1 ms	**25586.219 ms**	99047 ms	2209
10 ms	**308061.564 ms**	990893 ms	7015

Indexing Parameter QoS Delay (IP Spoof) standar TIPHON					
Testing Period (ms)	**Min (ms)**	**Max (ms)**	**Rata-rata (ms)**	**Indeks**	**Kategori**
0.010ms	0,024	1330,90	**119,095**	4	Sangat Bagus
0.100ms	0,020	6930,793	**1347,642**	1	Tidak Bagus
1 ms	0,027	95674,482	**22707,677**	1	Tidak Bagus
10 ms	0,022	983326,812	**260603,086**	1	Tidak Bagus
Rata-rata	0,023	271815,747	**71194,375**	1	Tidak Bagus

Selanjutnya pada data pengujian serangan IP Spoof pada host3, latency (delay) memiliki nilai minimal pada Testing

Period 0.010 millisecond (119,095 ms) dan nilai maksimal pada Testing Period 10 millisecond (71,194,375 ms). Ini menunjukkan bahwa selama serangan IP Spoof, kualitas komunikasi jaringan pada host3 dapat dikategorikan sebagai "Tidak Bagus" berdasarkan standar TIPHON dengan nilai Index 1, karena rata-rata delay packet data melebihi 450 ms.

H. Analisis Data Serangan Pada 10.1.1.5 (Host5)

Pada analisis data serangan pada Host 5 (10.1.1.5), Parameter delay diuji berdasarkan hasil pengamatan menggunakan command ping

Menurut analisa data pada tabel. Setelah terjadinya Relay Attack (Fake link), terjadi lonjakan pada delay(latency) yang terpapar pada tabel tersebut serta ditujukan adanya rata rata delay terendah ada pada pengujian dengan Testing Period 0.010 millisecond dengan latency 532.574 millisecond, serta adanya rata rata tertinggi ada pada pengujian dengan Testing Period 10 millisecond dengan latency 140.901 millisecond

Selanjutnya, dilakukan pendataan Latency(Delay) dari host2 ke host 5 pada serangan Flood IP Spoof, berikut

Ip spoofed Host 10.1.1.5			
Testing Period	**Host 10.1.1.5 (ms)**	**Durasi**	**Duplikasi**
0.010ms	532.574 ms	10066 ms	81
0.100ms	256.363 ms	10151 ms	92
1 ms	117.919 ms	99157 ms	99
10 ms	140.901 ms	990896 ms	99

terlampir tabel data hasil dari analisa latensi menggunakan ping:

Hasil pengujian latency(delay) dari serangan IP Spoofing pada host5 yang terpapar pada tabel. Setelah terjadinya IP Spoof, terjadi lonjakan pada delay(latency) yang terpapar pada tabel tersebut serta ditujukan adanya rata rata delay terendah ada pada pengujian dengan Testing Period 0.010 millisecond dengan latency 96.959 millisecond, serta adanya rata rata tertinggi ada pada pengujian dengan Testing Period 10 millisecond dengan latency 689.25 millisecond.

Indexing Parameter QoS Delay (Relay Attack) standar TIPHON					
Testing Period (ms)	**Min (ms)**	**Max (ms)**	**Rata-rata (ms)**	**Indeks**	**Kategori**
0.010ms	0,016	1779,741	532,574	1	Tidak Bagus

Relay Attack Host 10.1.1.5			
Testing Period	**Host 10.1.1.5 (ms)**	**Durasi**	**Duplikasi**
0.010ms	532.574 ms	10066 ms	81
0.100ms	256.363 ms	10151 ms	92
1 ms	117.919 ms	99157 ms	99
10 ms	140.901 ms	990896 ms	99

Indexing Parameter QoS Delay (Relay Attack) standar TIPHON					
Testing Period (ms)	**Min (ms)**	**Max (ms)**	**Rata-rata (ms)**	**Indeks**	**Kategori**
0.100ms	0,022	798,259	256,363	2	Sedang
1 ms	0,022	348,538	117,919	4	Sangat Bagus
10 ms	0,025	2365,157	140,901	4	Sangat Bagus
Rata-rata	0,021	1322,924	**261,939**	2	Sedang

Hasil pengujian Serangan Relay Attack pada Host5 menunjukkan rata-rata delay terendah terjadi pada Testing Period 1 milisecond (117,919 ms), sementara rata-rata tertinggi tercatat pada Testing Period 0.010 milisecond (532,574 ms). Berdasarkan standar TIPHON, kondisi komunikasi jaringan pada Host5 saat serangan Relay Attack dapat dikategorikan sebagai "Sedang" dengan nilai Index 2. Ini menunjukkan bahwa rata-rata delay data paket berada dalam kisaran 300 hingga 450 ms. Dengan demikian, selama serangan Relay Attack, kualitas layanan jaringan pada Host5 dapat dianggap sedang berdasarkan nilai delay yang diukur.

Indexing Parameter QoS Delay (IP Spoofing) standar TIPHON					
Testing Period (ms)	**Min (ms)**	**Max (ms)**	**Rata-rata (ms)**	**Indeks**	**Kategori**
0.010ms	0,010	1221,318	96,959	4	Sangat Bagus
0.100ms	0,020	1854,706	235,817	2	Sedang
1 ms	0,027	5981,826	376,362	2	Sedang
10 ms	0,022	6449,929	689,25	1	Tidak Bagus
Rata-rata	0,02	3876,945	**349,597**	2	Sedang

Dari data yang terpapar pada tabel, yang berisi data pengujian Serangan IP Spoof pada Host5, ditemukan bahwa rata-rata delay terendah terjadi pada Testing Period pengujian 0.010 milisecond (96,959 ms), sementara rata-rata tertinggi tercatat pada Testing Period 10 milisecond (689,25 ms). Menurut standar TIPHON, komunikasi jaringan pada Host5 selama terjadinya Serangan IP Spoof dapat dikategorikan sebagai kondisi "Sedang" dengan nilai Index 2. Ini menunjukkan bahwa rata-rata delay data paket berada dalam kisaran 300 hingga 450 ms. Dengan demikian, selama Serangan IP Spoof, kualitas layanan jaringan pada Host5 dapat dianggap sedang berdasarkan nilai delay yang diukur.

V. HASIL DAN PEMBAHASAN

Dari implementasi dan analisis serangan Relay Attack & IP Spoofing dalam eksperimen jaringan SDN dengan pendekatan PPDIOO, dapat diambil beberapa kesimpulan.

Pertama, Selama Serangan Relay Attack dan Serangan IP Spoofing, Host 3 mengalami delay buruk dengan delay rata-rata 83,832,547 ms (pada Relay Attack) dan 71,194,375 ms (pada IP Spoof) yang mana melebihi 450 ms sehingga terkategori sebagai "Tidak Bagus" dengan Indeks 1 berdasarkan TIPHON, sementara Host 5 mengalami delay sedang dengan delay rata-rata 261,939 ms (pada Relay Attack) dan 349,597 ms (pada IP Spoof) yang mana kedua kondisi ini masuk dalam rentang 300 hingga 450 ms yang terkategori "Sedang" dengan Indeks 2 berdasarkan standar yang digunakan yaitu TIPHON. Dengan demikian, dampak serangan pada Host 3 dan Host 5 memiliki tingkat delay yang berbeda..

Kedua, pada kedua serangan ini mengancam integritas dan kinerja jaringan SDN. Dalam hal efisiensi, Relay Attack dapat memanfaatkan lalu lintas komunikasi, sementara IP Spoofing memungkinkan serangan tanpa membutuhkan sumber daya yang kompleks.

Dan berdasarkan kesimpulan dari data hasil analisa kualitas jaringan antar Host 3 dan Host 5 setelah dilakukannya serangan, penulis menyimpulkan bahwa ada pengaruh yang besar dari jarak pada Host yang menyerang dengan keefektifan dampak yang terjadi pada Host lain di sebuah jaringan tersebut. Dalam kasus ini, Host 3 berdekatan dengan Host 1 yang juga tersambung oleh Host 2 yang mana secara tidak langsung dapat dikatakan Host 3 memiliki jarak yang lebih dekat dengan penyerang, karena penyerang berada di dalam switch yang sama dengan Host penyerang, yaitu Switch 2. Berbeda hal dengan Host 5 yang tersambung tidak terlalu dekat dengan Host penyerang, yang menjadikan kualitas jaringan pada Host 5 bisa dikatakan tidak terlalu buruk, dibandingkan dengan Host 3

Dari sudut pandang penyerang, analisis penelitian ini mengungkapkan wawasan yang berharga dalam melacak potensi kerentanan dalam perancangan jaringan SDN. Dalam penelitian ini, QoS hanya diukur melalui Latency (Delay). Penelitian berikutnya disarankan untuk mempertimbangkan variabel seperti throughput dan jitter untuk mengukur dampak Relay Attack & IP Spoofing secara lebih komprehensif pada kualitas jaringan.

Untuk penelitian selanjutnya dapat mengevaluasi efektivitas strategi perlindungan terhadap serangan Relay Attack dan IP Spoofing. Eksperimen saat ini hanya dilakukan dalam satu periode waktu tertentu, sehingga hasilnya dapat berbeda dalam waktu dan kondisi yang berbeda. Oleh karena itu, diperlukan pengambilan sampel yang lebih luas, termasuk pengambilan data pada berbagai waktu yang berbeda dan dalam berbagai kondisi jaringan internet, baik yang sibuk maupun normal. Hal ini akan membantu meningkatkan keakuratan dan validitas hasil penelitian.

REFERENSI

[1] B. Lin, X. Zhu, and Z. Ding, “Research on the Vulnerability of Software Defined Network,” 2017.

[2] J. Wang, Y. Tan, and J. Liu, “Topology poisoning attacks and countermeasures in SDN-enabled vehicular networks,” in *2020 IEEE Global Communications Conference, GLOBECOM 2020 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Dec. 2020. doi: 10.1109/GLOBECOM42002.2020.9348183.

[3] Y. Gao and M. Xu, “Defense Against Software-Defined Network Topology Poisoning Attacks,” 2023.

[4] G. Pickett and G. P. Com, “Abusing Software Defined Networks.”

[5] Jāmi‘at Qaṭar, Institute of Electrical and Electronics Engineers. Qatar Section., and Institute of Electrical and Electronics Engineers, *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) : February 2-5, Doha, Qatar.*

[6] F. Abazari, F. Esposito, H. Takabi, H. Hosseinvand, and T. Pecorella, “Teaching software-defined network security through malicious tenant detection,” *Internet Technology Letters*, vol. 2, no. 6. John Wiley and Sons Inc, Nov. 01, 2019. doi: 10.1002/itl2.131.

[7] P. Shrivastava, A. Agarwal, and K. Kataoka, “Poster: Detection of topology poisoning by silent relay attacker in SDN,” in *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*, Association for Computing Machinery, Oct. 2018, pp. 792–794. doi: 10.1145/3241539.3267763.

[8] N. E. Hastings, “TCP /IP Spoofing Fundamentals.”

[9] C. A. Joglekar, “Route Manipulation using SDN and Quagga,” 2017.