# Analisis Perbandingan Pengujian Distributed Denial of Service (DDoS) dan Rushing Attack pada Jaringan UDP dengan Routing AODV

**Ananda Ari Ramadhan[1], Dr. Maman Abdurohman, S.T, M.T.[2], Aji Gautama Putrada, S.T,M.T[3]**
[1,2,3]Prodi S1 Teknik Informatika. Fakultas Informatika, Universitas Telkom
[1]annndaari@gmail.com, [2]m_abdurohman@yahoo.com , [3] agp.sat@gmail.com

**Abstrak**

**Protokol UDP menjadi salah satu protokol yang banyak digunakan didunia saat ini dan menjadi salah satu protokol yang mendukung berjalannya komunikasi baik komunikasi suara maupun komunikasi data.Dengan semakin populer nya protokol ini semakin rentan pula jaringan ini mendapatkan serangan dari pihak yang tidak bertanggung jawab, serangan-serangan yang biasa terjadi pada jaringan adalah Distributed Denial of Service (DDoS), *Rushing Attack*, *BlackHole* dan sebagainya. Pada Tugas akhir ini akan membandingkan serangan yang kemungkinan besar dilakukan yaitu *Distributed Denial of Service* (DDoS) dan *Rushing Attack* pada protokol UDP dengan bantuan *routing* AODV.**

**Katakunci : DDoS,Rushing Attack,UDP,AODV, *Confidentiality, Integrity, Availability***

**Abstract**

**UDP protocol became one of the protocols that are widely used in the world today and be one of the protocols that support the communication goes both voice communications as well as its increasingly popular data.Dengan communication protocol is more vulnerable anyway this network under attack from those who are not responsible,common attack on the network is a Distributed Denial of Service (DDoS), Rushing attack, BlackHole and others.In this final project will compare the attacks were most likely to do is Distributed Denial of Service (DDoS) and Rushing Attack on the UDP protocol with AODV routing.**

**Keywords : DDoS,Rushing Attack,UDP,AODV, *Confidentiality, Integrity, Availability***

## 1. Pendahuluan

Manusia seiring dengan perkembangan zaman di era digital kebutuhan manusia untuk berkomunikasi semakin meningkat. Seperti kebanyakan orang saat ini perangkat yang digunakan adalah perangkat *handphone* yang digunakan untuk berkomunikasi via suara, data dan sebagainya. Teknologi komunikasi yang digunakan saat ini lebih di dominasi dengan penggunaan data internet baik dalam layanan *Voice Over, Video Stream*, dan lain lain Seperti yang sudah ketahui layanan-layanan semacam itu menggunakan jaringan UDP sebagai *background* jaringanya.

Dengan Teknologi UDP sendiri bukan teknologi yang amat baru. Teknologi ini sudah banyak digunakan dan diaplikasikan dalam kehidupan sehari-hari. Teknologi ini juga sudah didukung dengan berbagai macam *routing* protokol yang mendukung berjalan dengan baiknya teknologi ini, seperti *AODV, AOMDV*, dll. *Routing* protokol menjadi *support system* yang sangat berpengaruh dalam berjalananya jaringan ini oleh karena itu pemilihan *routing* menjadi faktor penting dalam sebuah jaringan. Namun dengan semakin banyak yang menggunakan UDP sebagai *background* jaringan, semakin banyak pula rentan jaringan ini mendapatkan serangan.

Kejahatan atau serangan yang mungkin dan sering terjadi pada layanan *mobile* berbasis UDP ini adalah *Distributed Denial of Service* (DDoS). Serangan ini akan menbanjiri jaringan yang ada dengan data, dan bila terus berlangsung lama dengan jumlah *flooder* semakin banyak dan terdistribusi maka performansi jaringan semakin lama akan semakin menurun dan tidak menutup kemungkinan hinggal menonaktifkan jaringan tersebut. Selain serang *DDoS* ada juga serangan yang tidak kalah berbahaya yaitu serangan *rushing attack*, serangan ini adalah serangan yang mengirimkan transmisi yang lebih besar berupa RREQ untuk mendapat prioritas jalur..

## 2. Dasar Teori

### 2.1 User Datagram Protocol

UDP, singkatan dari *User Datagram Protocol* adalah salah satu protokol dari7 *layer TCP/IP* yang mendukung komunikasi yang *unreliable* atau dengan kata lain tidak menjamin data sampai kepada destination atau penerima. Protokol UDP menjadi protokol yang tergolong hemat sumber daya baik memori maupun prosesor, beberapa layanan membutuhkan penggunaan protokol yang ringan yang dapat melakukan fungsi-fungsi spesifik dengan saling bertuar pesan, contoh layanan yang dimaksut adalah *Domain Name System*. Protokol ini dikenal dengan *connectionless* protokol ini tidak membutuhkan proses negosiasi atau mengetahui secara pasti antar node untuk bertukan informasi. Protokol ini dikenal juga *Unreliable* atau dengan kata lain jaringan ini tidak menjamin data yang di kirimkan dari pengirim ke penerima.

### 2.2 Ad hoc On-Demand Distance Vector Routing

*Ad hoc On-Demand Distance Vector (*AODV) adalah algoritma *routing* yang digunakan untuk *mobile* di jaringan *ad hoc*. *Routing* protokol ini menawarkan adaptasi cepat untuk kondisi *Dynamic Link*, pemanfaatan memori yang rendah, pemanfaatan jaringan yang rendah dan banyak memanfaatkan *unicast*. *Routing* ini menggunakan urutan nomor tujuan untuk memastikan *node* pada *loop* nya.Pada Routing protokol ini mengenal *Route Request* (RREQs) , *Route Replies* (RREPs), dan *Route Errors* (RERRs) pesan-pesan ini di terima melalui protokol UDP dan *IP header*. *Routing* ini berperan sangat penting apabila rute dari pengirim menuju tujuan tidak ditemukan atau memerlukan rute baru, maka *routing* ini akan mengirimkan RREQ ke semua agar mengetahui jalur yang akan dibuat. Namun apabila jalur sudah ada routing ini tidak terlalu diperlukan [1].

### 2.3 Distributed Denial of Service (DDoS)

*Distributed Denial of Service* (DDoS) adalah serangan dari *Denial of Service* (DoS) yang lebih massive atau dengan kata lain serangan DoS yang tersebar dimana penyerang memiliki satu atau lebih unik IP address yang digunakan untuk membanjiri suatu layanan. Serangan ini biasanya banyak digunakan untuk melakukan tindakan kriminal , dimana mereka melakukan serangan ini untuk memeras penyedia layanan.

Serangan DDoS secara sederhana melakukan apa yang di lakukan oleh DoS
namun pada serangan ini ada yang disebut zombie, zombie ini adalah para penyerang yang sudah di *setting* untuk melakukan serangan dalam satu waktu dan bersama-sama dengan mengalirkan data yang sangat besar dengan tujuan untuk menunkan kualitas jaringan bahkann untuk menonaktifkan suatu jaringan [2].

### 2.4 Rushing Attack

*Rushing Attack* adalah sebuah serangan jaringan dimana pada serangan ini melakukan duplikasi secara cepat dengan transmisi yang lebih tinggi untuk mengacaukan jaringan dan mendapatkan forward akses lebih dibanding dengan node yang lain [3].

Ketika node mengirimkan paket untuk permintaan route atau RREQ ke *node* lain dalan jaringan wireless, jika ada *node rushing* maka node ini akan menerima paket RREQ dan mengirim kembali ke tetangganya dengan transmisi yang lebih tinggi dibandingkan dengan *node* yang lain. Karena tranmisi yang lebih tinggi ini penyerang akan tiba terlebih dahulu di *node* tujuan dan *node* tujuan akan menerima paket RREQ ini dan membuang paket RREQ yang lain.

### 2.5 Packet Delivery Ratio

*Packet Delivery Ratio* adalah rasio dari berapa banyak packet yang diterima oleh penerima dengan total yang paket yang di kirim oleh pengirim adalah periode waktu tertentu.

$$\text{Packet Delivery Ratio} = (Ri/Si) \times 100\% \quad (1)$$

Dimana Ri adalah total paket data yang diterima, Si adalah total paket daya yang dikirim [3].

### 2.6 Throughput

*Throughput* adalah rata-rata rate paket data per detik yang berhasil di terima melewati jaringan *channel* [3].

$$\text{Throughput} = (Pi/T) \quad (2)$$

Dimana Pi (bit) adalah rata-rata jumlah paket yang diterima dan T (detik) adalah rata-rata waktu transmisi.Throughput sendiri adalah kecepatan transfer data efektif dalam kbps.

### 2.7 Network Security

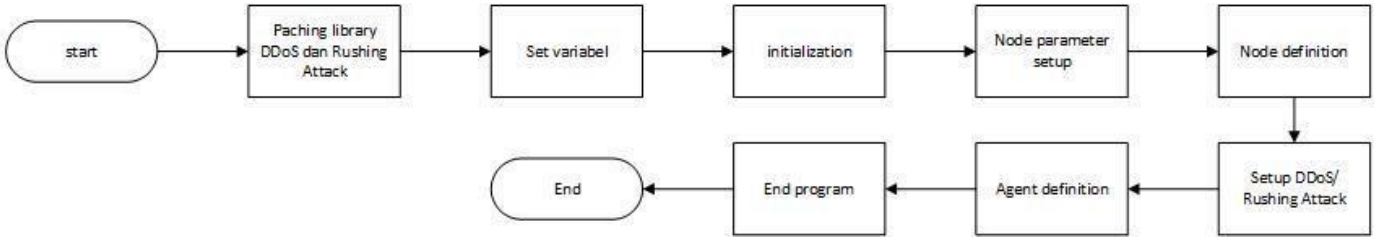
*Confidentiality*, *Integrity*, dan *availability* atau sering juga disebut dengan CIA triad , adalah model design untuk memandu keaman jaringan. *Confidentiality* bertujuan untuk mengatur keterbatasan akses informasi pada data didalam jaringan, *integrity* bertujuan untuk menjamin informasi terpercaya dengan akurasi yang baik dan yang terakhir *availability* bertujuan untuk menjamin ketersediaan jaringan saat dibutuhkan dan digunakan oleh pihak-pihak yang terpercaya [5].

Pada model keamanan jaringan ini atau CIA ketiga unsur ini menjamin keamanan jaringan yang ada, oleh sebab itu unsur ini yang nantinya akan dijadikan analisis dalam proses penarikan kesimpulan.

## 3. Pembahasan

### 3.1 Gambaran Umum Sistem

Adapun gambaran umum pada perancangan sistem berisikan dua tipe topologi jaringan untuk *Distributed Denial of Service* (DDoS), *Rushing Attack* dan *flowchart* yang menggambarkan tahapan penelitian yang dilakukan dalam penyusunan tugas akhir, yaitu:




Gambar 1 Flowchart sistem

Simulasi ini di mulai dengan *Paching library* pada NS2 lebih tepatnya pada NS2 AODV *library* , baik pada AODV.cc atau AODV.h , setelah itu harus dilakukan *running* untuk meng-*update library* yang sudah di *paching* sebelumnya . Selanjutnya pembuatan main.tcl untuk membuat topologi dan mendefinisikan jaringan yang akan kita buat.

Setelah pembuatan .tcl tahap selanjutnya set variabel yang akan digunakan nantinya pada jaringan yang akan dilakukan pengujian, lantas lakukan inisialisasi untuk membuat simulator pada NS2. *Setup Node* Parameter ditujukan untuk men-set parameter apa saja yang akan ada dalam *node*, karena pada penelitian ini *node* tidak bergerak kita tidak perlu melakukan *setting* pergerakan *node*. Setelah itu *setting* untuk *node* yang akan dijadikan *flooder* pada DDoS atau sebagai *node Rushing.*

Tahap selanjutnya kita menentukan *udp agent dan udp null*, atau dengan kata lain *setting udp sender dan udp receiver*, besaran paket yang dikirimkan, waktu dimulainya pengiriman paket dan waktu berhentinya pengiriman paket. Diakhiri dengan prosedur untuk menjalankan simulasi dan mengakhiri simulasi. Adapun parameter yang digunakan dalam simulasi ini sebagai berikut :

Tabel 1 Parameter Simulasi

| Parameter | Value |
|---|---|
| Channel Type | Wireless Channel |
| Propagation | Two Ray Ground |
| Routing Protocol | AODV |
| Queueing Method | Droptail |
| Total Node | 30 |
| Topography | 1000x1000 |
| Simulation Time | 100 Second |
| Traffic Type | UDP |
| Attack Type | DDoS and Rushing Attack |
| Antena Type | Omni Directional |
| MAC type | IEEE 802.11 |

### 3.2 Hasil dan Analisis Pengujian

Pengujian yang dilakukan oleh penulis dilakukan dengan bantuan Network Simulator 2 (NS2) ditujukan untuk mendapatkan data *packet send, packet receive, packet delivery ratio*, dan *average throughput,* dengan beberapa skenario yaitu :

i. Pengujian jaringan Benchmark
ii. Pengujian serangan DDoS
*iii.* Pengujian serangan Rushing Attack

Dari 3 skenario di atas pertama dilakukan pengujian jaringan benchmark sebagai jaringan patokan saat jaringan tidak dilakukan serangan apapun, data yang diperoleh pada jaringan nantinya akan di bandingkan dengan skenario lain. Setelah mendapatkan data pembanding dilakukan skenario ke 2 yaitu jaringan yang diserang dengan serangan DDoS, serangan ini memiliki 10 *flooder* atau 10 penyerang yang akan diuji sebanyak jumlah *flooder*nya. Selanjutnya pada pengujian ke 3 dilakukan pengujian jaringan pada serangan

*rushing attack* , dengan jumlah *node flooder* sebanyak 10 dan dilakukan pengujian sebanyak jumlah *node rushing* , adapun hasil pengujian sebagai berikut:

Tabel 2 Hasil Pengujian Tanpa Serangan

| Pengujian | Send Packet | Receive Packet | Drop Packet | Average Throughput (kbps) | Average Latency (ms) | Packet Delivery Ratio (%) | Average Packet Loss (%) |
|---|---|---|---|---|---|---|---|
| 1 | 2882 | 2872 | 8 | 229.94 | 244,577 | 99,7224 | 0,277585 |
| 2 | 2882 | 2880 | 2 | 210.44 | 129,035 | 99,93 | 0,07094 |
| Avg | 2882 | 2876 | 5 | 220,19 | 186,806 | 99,8262 | 0,1792625 |

Dari data pengujian untuk skenario 1 yaitu jaringan yang tidak terdampak serangan *DDoS* maupun *Rushing Attack*, pada jaringan ini *packet* yang terkirim dari 2 kali percobaan sama besar nya yaitu 2882 paket, sedangkan paket yang diterima berubah. Pada percobaan pertama paket yang diterima oleh penerima sebesar 2872 dan pada percobaan kedua paket yang diterima sebesar 2880 dengan rata-rata paket yang diterima sebesar 2976 dan nilai ini yang akan menjadi acuan dalam pengujian selanjutnya, dari perbandingan paket yang di kirim dengan paket yang diterima terdapat perbedaan. Pada percobaan pertama 8 buah paket tidak dapat diterima oleh penerima sedangkan pada percobaan ke-2 3 buah paket tidak diterima oleh penerima. Dengen adanya paket yang tidak diterima oleh penerima artinya *Packet Delivery Ratio* pada percobaan ini tidaklah 100%

*Packet Delivery Ratio* pada percobaan pertama sebesar 99,72% sedangkan pada percobaan ke-2 *Packet Delivery Ratio* sebesar 99,93% dengan rata-rata 99,82% nilai ini yang nantinya menjadi nilai acuan dalam percobaan selanjutnya.Sedangkan pada nilai *throughput* pada percobaan ke-1 sebesar 229,94 kbps dan bernilai 210,4 kbps pada percobaan ke-2, rata-rata pada throughput ini juga yang menjadi acuan pada perucobaan selanjutnya sebesar 220,19 kbps.

Pengujian yang dilakukan pada skenario ini di bagi menjadi 2 bagian pertama pengujian jaringan dengan serangan DDoS dengan *flooder* yang bertambah dari 1 hingga 10, lalu pengujian kedua pada jaringan dengan serangan *Rushing Attack* dengan penyerang dari 1 hinggal 10. Berikut hasil dari pengujian dengan DDoS yang akan ditampilkan pada tabel di bawah :

Tabel 3 Hasil Pengujian dengan DDoS

| Flooder | Send Packet | Receive Packet | Drop | Avg Throughput (kbps) | Avg Latency (ms) | Packet Delivery Ratio(%) | Avg Packet Loss(%) |
|---|---|---|---|---|---|---|---|
| 1 | 2882 | 2653 | 244 | 212.29 | 1100,07 | 92,0541 | 8,46634 |
| 2 | 2882 | 2261 | 648 | 181.00 | 1027,23 | 78,4525 | 22,4844 |
| 3 | 2882 | 1820 | 1093 | 145.64 | 1423,22 | 63,150 | 37,9251 |
| 4 | 2882 | 1379 | 1552 | 110.49 | 1321,7 | 47,8487 | 52,8105 |
| 5 | 2882 | 815 | 1943 | 71.73 | 1613,71 | 28,279 | 67,279 |
| 6 | 2882 | 600 | 2217 | 49.14 | 2158,73 | 20,8189 | 76,9257 |
| 7 | 2882 | 337 | 2423 | 36.50 | 900,985 | 11,6933 | 11,6933 |
| 8 | 2882 | 231 | 2530 | 21.21 | 1708,01 | 8,01527 | 87,7863 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 9 | 2882 | 81 | 2736 | 9.06 | 2543 | 2,81055 | 94,9341 |
| 10 | 2882 | 70 | 2756 | 7.31 | 506,933 | 2,42887 | 95,628 |

Dari hasil pengujian pada jaringan yang dilakukan serangan *DDoS* , dengan jumlah *node flooder* yang bertambah mulai dari 1 hinggal 10 *flooder*. Pada *flooder* yang berjumlah 1 jaringan sudah mulai terdampak dari serangan *DDoS* dimana *flooder* membanjiri jaringan dengan paket RREQ. Dari jumlah paket yang dikirimkan sebesar 2882 hanya 2653 paket yang dapat diterima dengan 244 paket yang drop, dan hampir semua parameter pengujian terjadi penurunan kualitas jaringan seperti *throughput* pada jaringan normal sebesar 220,19 kbps sedangkan saat dilakukan *DDoS* menjadi 212,29 kbps yang berarti serangan dengan *DDoS* cukup berpengaruh terhadap kualitas jaringan.
Sama halnya dengan *Packet Delivery Ratio* terjadi perubahan yang cukup signifikan dibandingkan dengan keadaan jaringan tanpa serangan. Pada jaringan yang telah terdampak serangan ini jumlah *Packet Delivery Ratio* menjadi 92,05% sedangkan pada jaringan normal sebesar 99,8% yang artinya terjadi penurunan yang cukup besar pada *Packet Delivery Ratio*.
Begitu pula dengan *flooder* berjumlah 2 hingga 10 buah *flooder* semakin banyak jumlah *flooder* makan semakin menurun pula kualitas jaringan, dan apabila *flooder* semakin banyak dan semakin masif tidak menutup kemungkinan jaringan ini tidak dapat digunakan atau *down*. Terbukti pada jumlah *flooder* sebanyak 10 buah, jaringan yang terdampak serangan *DDoS* jumah paket yang diterima oleh penerima hanya 70 sedangkan *drop packet* sebesar 2756 dengan jumlah yang sebesar itu artinya jaringan sudah tidak dapat menampung dengan baik atau mengakomodasi komunikasi dari pengirim kepada penerima. Presentasi *Packet Drop Ratio* juga semakin turun hanya sekitar 2,42% pada jumlah *flooder* sebesar 10, begitu pula dengan parameter yang lain *thourghput* pada jumlah *flooder* ini hanya 7 kbps yang berarti sangat kecil dan lambat. Berikut ini adalah pengujian selanjutnya dimana jaringan yang sama dipengaruhi serangan *Ruhsing Attack* :

Tabel 4 Hasil Pengujian dengan Rushing Attack

| Node RA | Send Packet | Receive Packet | Drop | Avg Throughput (kbps) | Avg Latency (ms) | Packet Delivery Ratio (%) | Avg Packet Loss (%) |
|---|---|---|---|---|---|---|---|
| 1 | 2882 | 2776 | 108 | 113.73 | 519,095 | 96,322 | 3,7474 |
| 2 | 2882 | 2667 | 195 | 109.25 | 1220,12 | 92,5399 | 6,76613 |
| 3 | 2882 | 2758 | 112 | 112.97 | 1060,36 | 95,6974 | 3,88619 |
| 4 | 2882 | 2449 | 361 | 102.37 | 1285,22 | 86,7106 | 12,526 |
| 5 | 2882 | 2722 | 137 | 111.50 | 1467 | 94,4483 | 4,75364 |
| 6 | 2882 | 2469 | 405 | 101.17 | 661,423 | 85,6697 | 14,0527 |
| 7 | 2882 | 2720 | 141 | 111.44 | 1113,8 | 94,3789 | 4,89244 |
| 8 | 2882 | 2684 | 177 | 109.97 | 1165,59 | 93,1298 | 6,14157 |
| 9 | 2882 | 2740 | 100 | 112.23 | 1398,74 | 95,0729 | 3,4981 |
| 10 | 2882 | 2721 | 128 | 111.46 | 1633,78 | 94,4136 | 4,44136 |

Pada pengujian dengan serangan Rushing Attack dengan jumlah *node* yang bertambah dari 1 hingga 10 buah *node rushing* kualitas jaringan cenderung menurun. Pada jumlah *node rushing* 1 paket data yang dikirimkan dari pengirim sebesar 2882 sedangkan paket yang diterima sebesar 2776 terdapat 108 paket yang drop dengan *throughput* sebesar 113,73 kbps dan *Packet Delivery Ratio* sebesasr 96,32%. Dan bertambah pada jumlah *flooder* sebanyak 2 *node rushing* paket yang dikirimkan sebanyak 2882 dengan paket yang diterima sebanyak 2667 dengan drop sebanyak 195 dan *throughput* sebesar 109,25 kbps lebih besar dari node rushing sebanyak 1 node sedangkan *Packet Delivery Ratio* sebesar 92,53%.
Namun pada jumlah *node* sebanyak 3 buah ada peningkatan kualitas jaringan dapat dilihat dari jumlah paket yang diterima lebih banyak dari jumlah 2 *node rushing* dari paket data yang dikirim sebanyak 2882 data sedangkan data yang diterima 2758 dengan data yang drop sebesar 112 *packet drop ratio* 95,69% dan *throughput* sebesar 112,97 kbps yang artinya lebih sedikit atau membaik dari jumlah 2 node rushing.

Hal ini juga terjadi pada jumlah *node attacker* berjumlah 4,5,6 dan 7, terjadi perbedaan yang sangat signifikan dari jumlah node tersebut pada jumlah *node rushing* sebanyak 4 *node rushing* yang dikirimkan sebesar 2882 sedangkan node yang di terima sebanyak 2449 dengen drop 361 dengan througput 102,37 kbps dengan *Packet Delivery Ratio* sebesar 86,71% .

Sedangkan dengan jumlah *node rushing* yang lebih banyak yaitu 5 *node rushing* kualitas jaringan cenderung membaik dari pada jumlah *rushing node* berjumlah 4 , terlihat pada paket yang di kirimkan sebesar 2882 dan yang di terima 2722 dengan drop paket sebanyak 137 . Namun besaran *througput* terlihat lebih besar dibandingkat yang sebelumnya menjadi 111,50 kbps dengan *Packet Delivery Ratio* sebesar 94,44% yang lebih membaik dari jumlah node sebelumnya.

Hal ini dapat terjadi dikarenakan faktor-faktor ini antara lain seperti letak *node* pengirim dan *node* penerima, jumlah *node rushing* dan letak *node rushing*, juga seberapa jauh jangkauan sebuah *node* dalam mengirim RREQ untuk mengetahui *node* tetangganya. Apabila *node* pengirim mengirimkan sinyal yang dikirimkan dan menjangkau *node* penerima maka *node* pengirim akan langsung mengirim paket langsung ke *node* tujuan tanpa perantara, tapi sebaliknya apa bila *node* penerima di luar langkauan *node* pengirim, maka *node* pengirim akan mengirimkan paket kepada *node* tetangga nya untuk di teruskan kepada *node* tujuan.

Analisis serangan *DDoS* dan *Rushing Attack* terhadap keamanan jaringan ini bertujuan untuk membandingkan serangan mana yang lebih berbahaya terhadap jaringan. Seperti yang sudah di bahas pada bab 3 tentang kemanan jaringan, kemanan jaringan memiliki 3 prinsip utama yaitu *Confidentiality, Availablelity, dan intergrity*. Masing-masing prinsip kemanan ini sendiri menjamin aspek kemanan dalam sebuah jaringan.

Serangan *DDoS* adalah serangan dengen membanjiri jaringan dengan data, pada kasus ini data yang di banjiri adalah RREQ atau *routing request* pada jaringan, serangan ini sangat berdampak pada jaringan dan menurunkan kualitas jaringan, pada serangan yang lebih masif jaringan akan *down* atau tidak dapat digunakan. Apabila jaringan tidak dapat digunakan atau kualitas jaringan yang menurun dengan drastis , prinsip *availability* dapat kita analisis pada serangan ini. Prinsip *integrity* dan *confidentiality* tidak terpengaruh dengan serangan ini karena serangan ini tidak merubah apapun dari data yang dikirimkan, hanya membanjiri jaringan dengan data. Artinya, Serangan *DDoS* ini sangan berdampak pada ketersediaan jaringan tertentu, tentunya ketersediaan ini menjadi sangat penting apabila jaringan digunakan untuk mengalirkan data-data yang penting seperti perbankan atau bisnis strategis lainnya.

Sedangkan serangan *Rushing Attack* adalah serangan dimana terdapat *node rushing* mengirimkan RREQ dengan transmisi yang lebih tinggi dibandingkan dengan *node* yang lain di dalam jaringan, dengan transmisi yang lebih tinggi ini *node reveicer* akan menerima paket dan membuang paket yang berasal dari node lain. Dengan kata lain *node rushing* sudah menguasai jalur dari *sender* menuju ke penerima. Pada *Rushing Attack* ini aspek *integrity* menjadi sangat berpengaruh karena *node rushing* dapat mempengaruhi data yang berjalan dengan kata lain jaringan disusupi oleh pihak yang tidak memiliki wewenang, hal ini dapat di manipulasi nantinya apa bila berjalan terus menerus. Selain itu, *Rushing Attack* juga sedikit berpengaruh kepada *availability* pada jaringan karena, dapat kita lihat dari hasil pengujian kualitas jaringan menurun walaupun tidak sebesar pada *DDoS* namun serangan ini cukup berpengaruh. Hal yang bisa sangat berpengaruh pada *Rushing Attack* dengan *availability* jaringan dikarenakan letak *node rushing* pada jaringan .

Apabila *node rushing* dekat dengan pengirim data efek yang di timbulkan tidak terlalu berpengaruh, sedangkan apabila *node rushing* terletak acak pada jaringan ini tidak telalu berefek besar pada namun apabila letak *node rushing* dekat dengan penerima efek yang ditimbulkan sangat besar.

## 4. Kesimpulan

Kesimpulan yang diperoleh dari tugas akhir ini adalah sebagai berikut :

1. Ditinjau dari pengujian dan analisis pada penelitian ini serangan *DDoS* jauh lebih berbahaya dari serangan *Rushing Attack* berdasarkan performa jaringan.
2. *Packet Delivery , Throughput* dan *Packet Delivery Ratio, DDoS* jauh lebih berpengaruh pada jaringan dibandingkan Rushing Attack
3. Letak *Node Rushing* berpengaruh besar pada performa Rushing Attack.
4. Ditinjau dari prinsip-prinsip keamanan *Rushing Attack* lebih berbahaya dibandingkan *DDoS* karena aspek *Integrity* dan *Availability*.

## Daftar Pustaka

[1] C. a. B.-R. E. a. D. S. Perkins, “Ad hoc on-demand distance vector (AODV) routing,” 2003.

[2] "Performance analysis of AODV routing protocol in MANET under the influence of routing attacks," dalam *Electrical and Information Technologies (ICEIT), 2016 International Conference on*, IEEE, 2016, pp. 536--542.

[3] M. R. a. o. Rifquddin, "Performance of AOMDV routing protocol under rushing and flooding attacks in MANET," dalam *2015 2nd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, IEEE, 2015, pp. 386--390.

[4] S. Shrivastava, "Rushing Attack and its Prevention Techniques," *International Journal of Application or Innovation in Engineering \& Management*, vol. 2, pp. 453--456, 2013.

[5] M. Rouse, "Whatls.com," 2017. [Online]. Available: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA.

[6] H. a. E.-r. M. a. M. H. a. E. H. B. Moudni, "Performance analysis of AODV routing protocol in MANET under the influence of routing attacks," dalam *Electrical and Information Technologies (ICEIT), 2016 International Conference on*, IEEE, 2016, pp. 536--542.

[7] S. M. a. B. G. R. Hussain, "Impact of DDoS attack (UDP Flooding) on queuing models," dalam *Computer and Communication Technology (ICCCT), 2013 4th International Conference on*, IEEE, pp. 210--216.

[8] M. a. M. Y. Yoshimachi, "A new AODV route discovery protocol to achieve fair routing for mobile ad hoc networks," dalam *Information Communication and Management (ICICM), International Conference on*, IEEE, 2016, pp. 222--226.

[9] "Performance Evaluation of Byzantine Rushing Attack in ADHOC Network," *International Journal of Computer Applications*, vol. 123, no. Foundation of Computer Science, 2015.