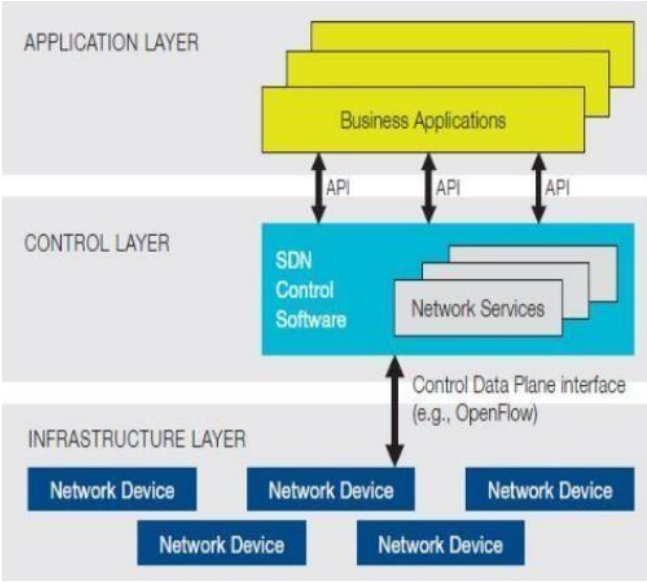
BAB I PENDAHULUAN

I.1 Latar Belakang

Teknologi pada saat ini semakin terus berkembang. Seiring berkembang pesatnya teknologi, diiringi dengan pesatnya jumlah *user* dan *hardware* yang membuat jaringan konvensional bersifat tidak fleksibel dan efisien untuk dilakukan integrasi terhadap jaringan terbaru. Dalam pengoperasiannya, jaringan tradisional bukan merupakan program yang mudah untuk di lakukan program ulang. Hal tersebutlah yang membuat para peneliti, mengembangkan teknologi terbaru pada jaringan yang terintegrasi dan berbasis *software* (Sanubari, 2019)



Gambar I. 1 Layer pada SDN (Saputra, Negara, Sanjoyo, 2018)

Software Defined Network (SDN) merupakan paradigma jaringan baru yang bertujuan untuk mengubah arsitektur jaringan. Pada jaringan SDN sangat mungkin untuk *administrator* melakukan penyediaan jaringan dengan cepat tanpa perlu mengkonfigurasi jaringan secara manual. Dengan cara yaitu memisahkan antara *control plane* dengan *data plane.* pada SDN *administrator,* tidak perlu mengkonfigurasi perangkat jaringan satu persatu yang sudah ada. Dikarenakan dengan adanya SDN, *administrator* memperoleh kontrol secara penuh pada keseluruhan jaringan di satu titik yang berguna untuk melakukan penyederhanaan terhadap pengoperasian jaringan. (Afif, Sukarno, Nugroho, 2018)

SDN memiliki 3 layer utama yaitu *Application Layer, Control Layer, dan*

Infrastructure layer. Pada bagian *Control layer.* Merupakan bagian inti pada SDN sebab, *control layer* bertugas untuk mengelola arus lalu lintas pada paket jaringan, kemudian meneruskan paket, dan melakukan pengambilan keputusan terkait perutean, berdasarkan *programming.* Penjelasan singkatnya yaitu *controller* memberikan kebijakan tinggi serta memisahkannya menjadi kebijakan rendah yang akan di install pada *switch,* lalu *switch* bertugas untuk meneruskan paket sesuai kebijakan yang telah ditetapkan oleh *controller.* Sehingga SDN dapat melakukan perancangan, kemudian membangun, hingga mengelola jaringan yang besar. Untuk mengelola jaringan yang besar terdapat beberapa tantangan yang harus dipertimbangkan Ketika melakukan penerapan SDN yaitu mengenai *availability, performance, scalability, dan security.* (Panjaitan, Sukarno, Nugroho, 2018)

Konsep pada jaringan SDN memiliki kelebihan dan kekurangan, pada segi kelebihannya yaitu memudahkan pengembangan serta eksperimen pada protokol yang baru, mudah dikelola dan memudahkan jaringan Ketika beradaptasi saat terjadi perubahan infrastruktur. (Ramadhan, Primananda, Yahya, 2018) Sedangkan dari segi kekurangan yang terdapat pada SDN yaitu dari *control plane* nya itu sendiri, dikarenakan SDN merupakan jaringan yang bersifat tersentralisasi. (Saputra, Negara, Sanjoyo, 2019) Selain itu, SDN memiliki kekurangan pada sistem algoritma nya, pada algoritma SDN memerlukan memori yang cukup besar untuk melakukan proses arahan agar berfungsi dengan baik. (Khairi, Ariffin, Muazzah, Latiff, 2021) pada sistemnya, SDN rentan terkena serangan seperti *Denial Of service (DoS)* dan *Defined Denial Of service (DDoS)* yang biasa melakukan serangan terhadap ketersediaan dari jaringan, sehingga pada jaringan tersebut tidak dapat menyediakan layanan atau tidak dapat melayani permintaan. (Putra, Negara, Yasirandi, 2021)

Pada kekurangan SDN disebutkan salah satu kekurangannya bahwa SDN rentan terhadap serangan DDoS, DDoS merupakan serangan yang terdistribusi yang mempunyai tujuan untuk menghabiskan bandwith atau sumber daya yang tersedia pada tujuan yang akan diserang dengan cara membanjiri server, jaringan yang bertautan, serta perangkat jaringan yang traffic nya tidak sah. (Sihombing,

Kartikasari, Bhawiyuga, 2019) Serangan DDoS biasanya memanfaatkan *protocol* UDP yang bersifat *connectionless* dengan tujuan untuk menyerang target. Kemudian paket data serangan lainnya juga banyak dikirimkan pada target yang akan diserang supaya paket tersebut bisa membanjiri komputer target. pada Sebagian kasus tertentu komputer berubah menjadi *hang* ketika paket data serangan tersebut dikirimkan (Yasin, Mohidin, 2018)

Untuk mengatasi permasalahan terkait serangan DDoS, pada tugas akhir ini akan merancang sistem deteksi DDoS menggunakan *Entropy* yang akan digunakan untuk melihat serangan yang terjadi pada SDN. Pada penelitian (Marilanda, Widiastuti, Sumadi, Nastiti, Faiqurrahman, 2019) menyebutkan bahwa *Entropy* merupakan metode yang digunakan dalam proses mendeteksi serangan DDoS dengan cara mengecek tingkat keacakan dari 250 paket pertama, dengan menyeleksi probabilitas kemunculan pada paket berdasarkan pada variabel yang terdapat pada IP sumber serta IP tujuan.

Berdasarkan penelitian tersebut, peneliti berinisiatif untuk meneliti terkait deteksi serangan DDoS pada SDN menggunakan metode *Entropy* dengan mencoba menambahkan apa yang telah peneliti (Marilanda, Widiastuti, Sumadi, Nastiti, Faiqurrahman, 2019) tambahkan serta mengembangkan penelitian dari (Sanubari, 2019) untuk mengembangkan nilai threshold dari peneliti tersebut untuk mendapatkan hasil akurasi tertinggi untuk deteksi menggunakan metode *entropy.*

I.2 Perumusan Masalah

Adapun perumusan masalah pada penelitian ini yaitu sebagai berikut:

1. Parameter apa saja yang digunakan untuk menentukan nilai *threshold* menggunakan metode *entropy*?
2. Fungsi nilai *threshold entropy* berguna untuk apa saja?
3. Darimana nilai *threshold entropy* didapatkan?
4. Berapa hasil akurasi tertinggi untuk deteksi serangan DDoS menggunakan metode entropy yang didapatkan pada penelitian ini?

I.3 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian ini yaitu sebagai berikut :

1. Mengetahui parameter apa saja yang digunakan untuk menentukan nilai *threshold* pada *entropy.*
2. Mengetahui fungsi nilai threshold pada metode entropy.
3. Mengetahui nilai threshold entropy pada penelitian ini berasal didapatkan.
4. Mengetahui hasil hasil akurasi tertinggi untuk deteksi serangan DDoS menggunakan metode entropy yang didapatkan pada penelitian ini.

I.4 Batasan Masalah

Adapun batasan – batasan terhadap penelitian ini adalah sebagai berikut :

1. Sumber data pada penelitian ini diambil dari dataset yang telah di*generate.*
2. Metode evaluasi penelitian ini menggunakan metode PPDIO

I.5 Manfaat Penelitian

Manfaat penelitian ini:

1. Bagi Universitas Telkom, penelitian ini bermanfaat dalam meningkatkan segikeamanan jaringan untuk mengantisipasi berbagai serangan yang ada.
2. Bagi peneliti lain yang bergerak dalam bidang keamanan jaringan, penelitian ini dapat berguna untuk mengembangkan penelitian mengenai *Entropy* pada *software defined network* yang telah ada.