IDENTIFIKASI SERANGAN DDOS SYN FLOOD MENGGUNAKAN ARTIFICIAL IMMUNE SYSTEM

TUGAS AKHIR

OLEH:

RIDHO ILHAM RENALDO

09011181520021

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

TAHUN 2020

HALAMAN PENGESAHAN

IDENTIFIKASI SERANGAN DDOS SYN FLOOD MENGGUNAKAN ARTIFICIAL IMMUNE SYSTEM

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana

OLEH :

Ridho Ilham Renaldo

09011181520021

Indralaya, Februari 2020

Pembimbing I,

Deris Stiawan, M.T., Ph.D.
NIP.197806172006041002

Pembimbing II,

Ahmad Heryanto, S.Kom.,M.T.
NIP.198701222015041002

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Pada hari Jumat tanggal 14 Februari 2020 telah dilaksanakan ujian sidang tugas akhir oleh Sarjana Ilmu Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Ridho Ilham Renaldo

NIM : 09011181520021

Judul : Identifikasi Serangan DDoS SYN Flood Menggunakan Artificial Immune System

Tim Penguji :

1. **Ketua**

   Adi Hermansyah, M.T. (.....)

2. **Penguji I**

   Dr. Reza Firsandaya Malik, M.T. (.....)

3. **Penguji II**

   Huda Ubaya, M.T. (.....)

Mengetahui,
Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama	: Ridho Ilham Renaldo
NIM	: 09011181520021
Jurusan	: Sistem Komputer
Judul Tesis	: Identifikasi Serangan DDoS SYN Flood Menggunakan Artificial Immune System

Hasil Pengecekan Software iThenticate/Turnitin : **3 %**

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil *penjiplakan / plagiat*. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, Februari 2020

Ridho Ilham Renaldo
NIM. 09011181520021

HALAMAN PERSEMBAHAN

" Don't give up when you still have something to give. Nothing is really over until the moment you stop trying" - Brian Dyson

Tugas Akhir ini saya persembahkan untuk :

- ***Kedua Orang tua dan Adik saya***
- ***Dosen Pembimbing dan Penguji***
- ***Sahabat – sahabat saya***
- ***Teman Seperjuangan Sistem Komputer 2015***
- ***Almamaterku***

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah SWT atas rahmat-nya sehingga penulis dapat menyelesaikan tesis yang berjudul **"*Identifikasi Serangan DDoS Syn Flood Menggunakan Artificial Immune System*"** di susun untuk memenuhi sebagian persyaratan kelulusan untuk memperoleh gelar Sarjana Komputer pada Jurusan Sistem Komputer Universitas Sriwijaya.

Pada kesempatan ini penulis menyadari keterbatasan dan kelemahan yang ada dalam menyelesaikan tesis ini sehingga penulis ingin menyampaikan ucapan terima kasih kepada pihak-pihak yang telah memberikan dukungan, bimbingan dan motivasi kepada penulis untuk menyelesaikan tugas akhir ini, kepada :

1. Allah SWT, yang telah memberikan rahmat dan karunia-Nya sehingga tugas akhir penulisan ini dapat berjalan dengan lancar.
2. Kedua orang tua beserta keluarga yang selalu mendoakan serta memberikan motivasi dan semangat.
3. Bapak Jaidan Jauhari, S.Pd, M.T selaku dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T., sebagai Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Bapak Deris Stiawan, M.T., Ph.D. dan Bapak Ahmad Heryanto, S.Kom., M.T selaku pembimbing yang telah meluangkan waktu, bantuan serta saran dan kritiknya dalam penyusunan tugas akhir ini.
6. Bapak Dr. Reza Firsandaya Malik, M.T. selaku Pembimbing Akademik Jurusan Sistem Komputer
7. Dosen-dosen pengajar yang telah memberikan ilmu bermanfaat kepada penulis selama menuntut ilmu di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya..
8. Mba Winda Kurnia Sari selaku Administrator Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya yang telah memberi kemudahan dalam pengurusan administrasi

9. Siti Dwi Oktariana Ningrum, S.SI. yang telah menyediakan waktunya dalam menemani, membantu dan memberikan semangat saya dalam menyelesaikan tugas akhir ini.
10. Kak Chandra Adi Winanto, S.Kom, Mbak Nurul Afifah, S.Kom., M.Kom. dan juga M. Ajran Saputra, S.Kom yang telah membantu saya dalam menyelesaikan tugas akhir ini.
11. Seluruh teman-teman Jurusan Sistem Komputer Angkatan 2015 yang telah membantu dan memberikan semangat pada masa-masa perkuliahan.
12. Semua pihak yang telah memberi dukungan kepada penulis dan tidak bisa disebutkan satu-persatu.

Akhir kata, penulis menyadari bahwa tugas akhir ini masih banyak kekurangan baik dari isi maupun susunan. Semoga tugas akhir ini dapat bermanfaat untuk kita semua.

Indralaya, Februari 2020

Penulis

IDENTIFIKASI SERANGAN DDOS SYN FLOOD MENGGUNAKAN ARTIFICIAL IMMUNE SYSTEM

Ridho Ilham Renaldo (09011181520021)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
E-mail : ridhoilhamr111@gmail.com

ABSTRAK

Serangan *Syn Flood DDoS* merupakan aktivitas serangan yang mengeksploitasi proses *three way handshake* pada koneksi TCP yang memanfaatkan *Hping3.* Sebagai tools yang untuk membuat traffic data serangan Syn Flood DDoS yang terdiri dari tiga skenario pembuatan dataset sehingga mendapatkan dataset yang bersifat homogen. *Algoritma Dendritic Cell* atau dikenal dengan DCA merupakan algoritma yang dirancang sebagai deteksi anomali pada traffic jaringan. Pada penelitian ini, serangan Syn Flood dapat diatasi menggunakan *Artificial Immune System* (AIS) dengan pemanfaatan *Algoritma Dendritic Cell*. Hasil dari deteksi *Artificial Immune System* (AIS) dengan pemanfaatan *Dendritic Cell Algorithm* (DCA) telah berhasil mendeteksi Serangan *DDoS SYN Flood* dengan tingkat akurasi 98,04 %, TPR 97,05 %, TNR 98,48 %, FPR 1,51% dan TNR 2,94%.

Kata Kunci : *Distributed Denial of Service*, *Syn Flood*, *Artificial Immune System, Dendritic Cell Algorithm*

IDENTIFACTION OF DDOS SYN FLOOD ATTACK BASED ON ARTIFICIAL IMMUNE SYSTEM

Ridho Ilham Renaldo (09011181520021)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
E-mail : ridhoilhamr111@gmail.com

ABSTRACT

Syn Flood DDoS attack is an attack activity that exploits a three way handshake process on a TCP connection that utilizes the *Hping3* tools to create data traffic for the *Syn Flood DDoS* attack which consists of three scenarios for creating a dataset to get a homogeneous dataset. *Dendritic Cell Algorithm* is an algorithm designed as an anomaly detection on network traffic. In this study, Syn Flood attacks can be resolved using Artificial Immune System (AIS) by utilizing the *Dendritic Cell Algorithm*.The Performance of *Artificial Immune System* (AIS) detection by utilizing the Dendritic Cell Algorithm (DCA) has succeeded in detecting *DDoS SYN Flood* attacks with an accuracy rate of 98.04%, *TPR* 97.05%, *TNR* 98.48%, FPR 1.51% and TNR 2.94%.

Kata Kunci : *Distributed Denial of Service*, *Syn Flood*, *Artificial Immune System, Dendritic Cell Algorithm*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

BAB I. PENDAHULUAN

1.1.Latar Belakang

Intrusion Detection System atau IDS merupakan kombisi hardware software yang berperan sangat penting dalam memantau atau memonitoring jaringan dan juga sistem yang di lakukan *attacker* dari aktifitas malicious. IDS secara umum dibagi dalam dua katagori cara deteksi yaitu *misue detection* dan *anomaly detection*[1]. Deteksi serangan dengan mencari persamaan data yang diamati dengan tingkah laku serangan yang telah ditemukan sebelumnya disebut *Misuse detection*. Sedangkan *anomaly detection* dengan mendeteksi yang dibawa dari perilaku yang berbeda dan jarang dari perilaku normal.

Dalam melakukan teknik deteksi IDS tidak hanya menerapkan *General Method* seperti *Computional Method* dan *Signature Method* tetapi juga *Artifical intelligence*[2]. Dalam sistem IDS *Artifical Intellegence* terdapat perkembangan yang diterapkan juga seperti *Fuzzy Teory, Neural Network, Genetic Algorithm, Artifical Immune Theory* dan lainnya.

Distributed Denial of Service (DDoS) merupakan bentuk lain dari serangan *Denial of Service* (DoS) yang dilakukan melalui sejumlah mesin daripada hanya menggunakan satu mesin saja. Mesin-mesin yang berbeda ini sering disebut "Zombies" karena penyerang menggunakannya untuk melakukan serangan dengan atau tanpa persetujuan pemiliknya[3]. Contoh serangan DDoS adalah serangan *SYN Flood*, *Smurf*, *Trinoo*, *TFN*, *TFN2K*, *Trinity*, dan *Mastream*.

Survey dari lembaga Arbor'S pada tahun 2008, [4] Serangan SYN-Flooding, DNS-Flooding, dan SMURF attack diklasifikasikan sebagai serangan terbesar pada tahun tersebut yang menyerang situs-situs pemerintahan dan 76% diantaranya SYN Flooding. SYN Flooding terjadi ketika pengguna tidak dapat terhubung ke server yang ditargetkan karena sistem yang digunakan tidak dapat menangani semua permintaan yang ada[5].

Dalam penelitian[6] membahas tentang cara mendeteksi serangan *DDOS SYN Flooding* dengan melalukan *generate dataset* berdasarkan *simulasi* dengan menerapkan algoritma *Dendritic Cell Algorithm (DCA)*. Tetapi tidak terlihat melakukan perhitungan *ambang batas/ threshold* dan nilai *MCAV*

Selanjutnya[7] menerapkan *Dendritic Cell Algorithm* yang digunakan untuk mendeteksi dari serangan *HTTP Denial of Service (DoS)* dengan menggunakan tools *slowloris,* dimana serangan DoS dibuat dengan memanfaatkan tools slowloris. Dengan menghasilkan akurasi 82.7% dan Detection Rate 90.2%

Dari beberapa rujukan diatas, metode yang akan digunakan dalam mendeteksi serangan T*CP SYN Flooding Distributed Denial Of Services (DDOS)* dengan menggunakan metode *Dendritic Cell Algorithm (DCA)* untuk dapat mengenali pola serangan SYN Flooding dan membedakannya dengan pola data normal.

1.2.Tujuan

Adapun tujuan dari penelitian ini adalah :

1. Membedakan atribut paket data normal dan serangan *SYN Flood Distributed Denial of Services (DDoS)*.
2. Mengukur kinerja atau deteksi serangan *SYN Flood Distributed Denial of Services (DDoS* dengan algoritma *Dendritic Cell Algorithm (DCA)*

1.3.Manfaat

Adapun manfaat yang dapat diambil dari penelitian ini adalah :

1. Dapat mengenali atribut paket data serangan *SYN Flood DDoS*
2. Dapat membedakan atribut paket data normal dan paket data atribut *DDoS SYN Flood* menggunakan algoritma *Dendritic Cell Algorithm (DCA).*

1.4. Rumusan Masalah dan Batasan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka rumusan masalah dan batasan masalah yang ada pada tugas akhir ini adalah :

1.4.1. Rumusan Masalah

1. Bagaimana cara membedakan atribut paket serangan *SYN Flood DDoS* dengan menerapkan *Dendritic Cell Algorithm (DCA)* ?

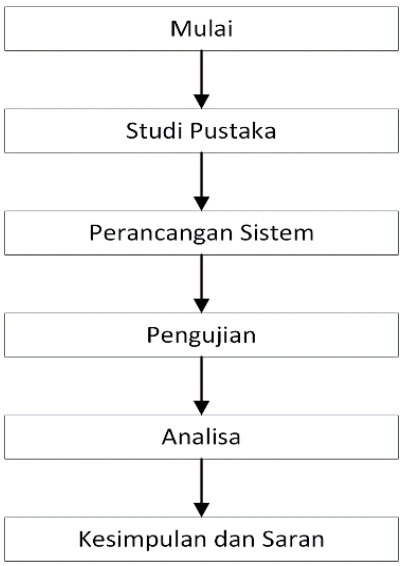
2. Bagaimana cara mengukur kinerja atau tingkat akurasi deteksi serangan *DDoS SYN Flood* yang didapat pada alert *SNORT* dengan yang didapatkan algoritma *Dendritic Cell Algorithm (DCA)* ?

1.4.2. Batasan Masalah

1. Dataset yang digunakan merupakan pada serangan *SYN Flood*
2. Dataset dikelompokan menjadi dua bagian yaitu data normal dan data serangan *SYN Flood*
3. Metode yang digunakan adalah *Dendritic Cell Algorithm*
4. Tidak dilakukan pada lalu lintas jaringan real-time
5. Tidak dilakukan pada lalu lintas jaringan yang terenskripsi
6. Tidak membahas bagaimana cara pencegahan serangan tersebut.

1.5. Metodologi Penelitian

Untuk memperoleh gambaran dalam penelitian ini, maka dituliskan metodologi penlitian yang berisi gambaran dalam setiap bab penelitian ini adalah :



Gambar 1.1 Metodologi Penelitian

1. Studi Pustaka (Tahap Pertama)

   Pada tahapan ini dengan mencari dan mempelajari literature dan referensi berupa *naskah ilmiah*, *buku* dan *mailing list* yang dapat menunjang metodologi dan pedekatan yang akan diterapkan pada penelitian.

2. Perancangan Sistem (Tahap Kedua)

   Tahap ini merupakan tahap dimana menentukan perangkat keras maupun perangkat lunak untuk merancang sistem dan kemudian merancangn topologi yang sesuai. Setelah itu langkah selanjutnya melakukan pengembangan yang telah dibahas sebelumnya.

3. Pengujian (Tahap Ketiga)

   Selanjutnya, dilakukan pengujian system dengan batasan masalah dengan parameter-parameter yang telah ditentukan.

4. Analisa (Tahap Keempat)

   Terakhir, menarik kesimpulan berdasarkan studi pustaka, hasil percancangan dan pegujian sistem dan analisa sistem dan juga dihadirkan saran dari penulis untuk penelitian selanjutnya.

4.1. Sistematika Penulisan

Agar memperoleh gambaran jelas mengenai penelitian ini, maka dibuatlah suatu sistematika penulisan yang berisi gambaran dalam tiap bab penelitian ini, yaitu:

BAB I. PENDAHULUAN

Bab ini berisi penjelasan secara sistematis mengenai landasan topik penelitian yang meliputi Latar Belakang, Tujuan, Manfaat, Rumusan Masalah dan Batasan Masalah kemudian Metodologi Penelitian, dan yang terakhir adalah mengenai Sistematika Penulisan.

BAB II. TINJAUAN PUSTAKA

Bab ini berisikan teori dari penelitan terkait dengan *Intrusion Detection System, SYN FloodDistributed Denial of Service attack*, *Dendritic Cell Algorithm (DCA),* yang berkaitan secara langsung dengan penelitian.

BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan secara sistematis, bagaimana proses penelitian dilakukan. Penjelasan pada bab ini meliputi tahapan perancangan sistem dan penerapan metode penelitian.

BAB IV. PENGUJIAN DAN ANALISA

Bab ini menjelaskan hasil pengujian yang dilakukan serta analisis dari tiap data yang diperoleh dari hasil pengujian.

BAB V. KESIMPULAN

Bab ini berisi kesimpulan tentang hasil penelitian yang telah dilakukan, serta menjawab setiap tujuan yang hendak dicapai sesuai yang tercantum pada BAB I (Pendahuluan)

DAFTAR PUSTAKA

[1] H. Choi, H. Lee, and H. Kim, "Fast detection and visualization of network attacks on parallel coordinates," *Comput. Secur.*, vol. 28, no. 5, pp. 276–288, 2009.

[2] Z. Ling, B. A. I. Zhong-ying, L. U. Yun-long, Z. H. A. Ya-xing, and L. I. Zhen-wen, "Integrated intrusion detection model based on artificial immune," *J. China Univ. Posts Telecommun.*, vol. 21, no. 2, pp. 83–90, 2014.

[3] S. Behal and K. Kumar, "Trends in Validation of DDoS Research," *Procedia Comput. Sci.*, vol. 85, no. Cms, pp. 7–15, 2016.

[4] K. Ramadhani, M. Yusuf, H. E. Wahanani, J. T. Informatika, and F. T. Industri, "Anomali Perubahan Traffic Jaringan Berbasis Cusum," *Comput. Secur.*, pp. 1–9, 2013.

[5] I. Publication, "International Journal of Computer Science & Information Security," *Comput. Networks*, vol. 9, no. 11, 2011.

[6] G. Ramadhan, Y. Kurniawan, C. Kim, A. T. C. P. Syn, and F. Ddos, "Design of TCP SYN Flood DDoS Attack Detection Using Artificial Immune Systems," pp. 72–76, 2016.

[7] C. Adi Winanto, "Deteksi serangan Denial of Service mengunakan Artificial Immune System," vol. 2, no. 1, pp. 1–67, 2017.

[8] R. Zhong and G. Yue, "DDoS detection system based on data mining," *Proc. Second Int.*vol. 1, pp. 62–65, 2010.

[9] A. Sanmorino and S. Yazid, "DDoS Attack detection method and mitigation using pattern of the flow," *2013 Int. Conf. Inf. Commun. Technol. ICoICT 2013*, pp. 12–16, 2013.

[10] K. R. W. V Bandara *et al.*, "Preventing DDoS attack using Data mining Algorithms," *Int. J. Sci. Res. Publ.*, vol. 6, no. 10, p. 390, 2016.

[11] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *Int. J. Distrib. Sens. Networks*, vol. 13, no. 12, 2017.

[12] P. Jongsuebsuk, N. Wattanapongsakorn, and C. Charnsripinyo, "Network intrusion detection with Fuzzy Genetic Algorithm for unknown attacks," *Int. Conf. Inf. Netw.*, pp. 1–5, 2013.

[13] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," *Comput. Networks*, vol. 31, no. 8, pp. 805–822, 1999.

[14] H. J. Liao, C. H. Richard Lin, Y. C. Lin, and K. Y. Tung, "Intrusion detection system: A comprehensive review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 16–24, 2013.

[15] A. Jamdagni, "Payload-based Anomaly Detection in HTTP Traffic," no. November, p. 172, 2012.

[16] S. Akbar, D. K. N. Rao, and D. J. A. Chandulal, "Intrusion Detection System Methodologies Based on Data Analysis," *Int. J. Comput. Appl.*, vol. 5, no. 2, pp. 10–20, 2010.

[17] D. Dasgupta, S. Yu, and F. Nino, "Recent advances in artificial immune systems: Models and applications," *Appl. Soft Comput. J.*, vol. 11, no. 2, pp. 1574–1587, 2011.

[18] L. Ding, F. Yu, and Z. Yang, "Survey of DCA for Abnormal Detection," vol. 8, no. 8, pp. 2087–2094, 2013.

[19] Z. Chelly and Z. Elouedi, “A survey of the dendritic cell algorithm,” *Knowl. Inf. Syst.*, vol. 48, no. 3, pp. 505–535, 2016.
[20] X. Zheng and Y. Fang, “Principle and Application of Dendritic Cell Algorithm for Intrusion Detection,” *Int. Conf. Signal Process. Syst.*, vol. 48, no. Icsps 2011, pp. 85–91, 2011.
[21] J. Greensmith, “The Dendritic Cell Algorithm,” *Thesis Degree Dr. Philos.*, no. October, pp. 1–316, 2007.
[22] E. A. Winanto, A. Heryanto, and D. Stiawan, “Visualisasi Serangan Remote to Local (R2L) Dengan Clustering K-Means,” *Annu. Res. Semin. 2016*, vol. 2, no. 1, pp. 359–362, 2016.
[23] K. Hafeez, M. Masood, O. Malik, and Z. Anwar, “LASSP: A logic analyzer for tweaking snort security and performance,” *Proc. - 2010 6th Int. Conf. Emerg. Technol. ICET 2010*, pp. 240–245, 2010.
[24] E. B. Susanto, “Evaluasi Hasil Klaster Pada Dataset Iris , Soybean-small , Wine Menggunakan Algoritma Fuzzy C-Means dan K-,” *Surya Inform.*, vol. 2, no. 1, pp. 6–13, 2016.
[25] S. Y. Wu and E. Yen, “Data mining-based intrusion detectors,” *Expert Syst. Appl.*, vol. 36, no. 3 PART 1, pp. 5605–5612, 2009.
[26] B. Yuwono, “Image Smoothing Menggunakan Mean Filtering, Median Filtering, Modus Filtering Dan Gaussian Filtering,” *Telematika*, vol. 7, no. 1, 2015.
[27] Z. Trabelsi, “Using Network Packet Generators and Snort Rules for Teaching Denial of Service Attacks,” no. July 2013, 2015.