DETEKSI SERANGAN *UDP FLOOD* MENGGUNAKAN METODE *RATE-BASED THRESHOLDING* PADA JARINGAN *LLN*

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

DISUSUN OLEH:

GHULAM ROBBANI TOHA
09011382025121

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2024

LEMBAR PENGESAHAN

Deteksi Serangan UDP Flood Menggunakan
Metode *Rate-Based Thresholding* Pada Jaringan LLN

Skripsi

Program Studi Sistem Komputer
Jenjang S1

Oleh:

Ghulam Robbani Toha
09011382025121

Palembang, 6 Januari 2025

Ketua Jurusan Sistem Komputer	Pembimbing Tugas Akhir
Dr. Ir. Sukemi, M. T.	**Huda Ubaya, S.T., M.T.**
NIP. 196612032006041001	**NIP. 198106162012121003**

AUTHENTICATION PAGE

DETECTION OF UDP FLOOD ATTACKS USING RATE-BASED THRESHOLDING METHOD ON LLN NETWORKS

THESIS

Dept. of Computer System

Bachelor's Degree

By:

Ghulam Robbani Toha

09011382025121

Palembang 6 January 2025

Head Of Computer System Department

Dr. Ir. Sukemi, M. T.

NIP. 196612032006041001

Supervisor

Huda Ubaya, S.T., M.T.

NIP. 198106162012121003

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Selasa

Tanggal : 24 Desember 2024

Tim Penguji

1. **Ketua : Aditya Putra Perdana Prasetyo, S.Kom., M.T**
2. **Penguji : Dr. Ahmad Zarkasi, M.T.**
3. **Pembimbing: Huda Ubaya, S.T., M.T.**

Mengetahui, 6/1/25

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M. T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Ghulam Robbani Toha
NIM : 09011382025121
Judul : Deteksi Serangan UDP *Flood* Menggunakan Metode *Rate-Based Thresholding* Pada Jaringan LLN.

Hasil Pengecekan Software iThenticate/Turnitin: 3%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam skripsi ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian, pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari siapapun.

Palembang, Januari 2025

Ghulam Robbani Toha
NIM.09011382025121

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Marilah kita panjatkan puji serta syukur atas kehadirat Allah SWT karena atas berkat hidayah dan karunia – Nya penulis dapat menyelesaikan penyusunan skripsi ini yang berjudul "**Deteksi Serangan UDP Flood Menggunakan *Metode Rate-Based Thresholding* Pada Jaringan LLN**"

Sebelumnya, penulis ingin memberikan serta mengucapkan terima kasih kepada beberapa pihak yang senantiasa memberikan ide, masukan, kritik, serta motivasi selama penulis melakukan penyusunan Tugas Akhir. Ucapan terima kasih tersebut ingin penulis sampaikan kepada :

1. Allah SWT yang senantiasa telah membberikan rahmat serta karunia – Nya sehingga penulis bisa menyelesaikan penulisan Tugas Akhir ini.
2. Orang tua saya tercinta Bapak Soepraptono dan Ibu Hayati Widaningsih yang tidak letih – letih dalam mengasuh serta mendidik saya sehingga saat ini dan tak ada hentinya juga dalam memberikan nasihat, semangat, serta juga dalam memberikan motivasi.
3. Bapak Prof. Dr. Erwin, S.Si, M.Si. yang merupakan Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. Sukemi, M.T., yang merupakan Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Huda Ubaya, M.T. selaku Dosen Pembimbing yang telah berkenan meluangkan waktu dan tenaga dalam membimbing, memberikan saran serta motivasi kepada penulis selama proses penulisan Tugas Akhir ini.
6. Bapak Iman Saladin B. Azhar S.KOM., M.MSI. selaku Dosen Pembimbing Akadamik Jurusan Sistem Komputer penulis saat ini.
7. Mbak Sari selaku admin jurusan Sistem Komputer yang telah berjasa dalam membantu permasalahan administrasi penulis.
8. Sahabat baik saya Sahara Diva Maharani, Siti Triwinarti Ningrum,Ully Afifa, Luqman Agus Dwiyono, M. Aziz Alhadi dan teman seperjuangan di Jurusan Sistem Komputer Unggulan 2020.

9. Seluruh pihak yang tidak dapat penulis sebutkan satu persatuyang telah memberikan doa dan bantuan dalam penyelesaian Tugas Akhir ini.
10. Almamater Universitas Sriwijaya.

Penulis menyadari bahwasannya Tugas Akhir yang telah diselesaikan ini masih tidak mendekati kata sempurna. Maka dari itu penulis meminta kritik, masukan, serta ide yang dapat digunakan oleh penulis agar penyusunan Tugas Akhir akan menjadi jauh lebih baik lagi di masa mendatang.

Wassalamualaikum Warahmatullahi Wabarakatuh

Palembang, Januari 2025
Penulis

Ghulam Robbani Toha
NIM. 09011382025121

DETEKSI SERANGAN *UDP FLOOD* MENGGUNAKAN METODE *RATE-BASED THRESHOLDING* PADA JARINGAN *LLN*

Ghulam Robbani Toha (09011382025121)
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : ghulam.toha@gmail.com

ABSTRAK

Kemajuan *Internet of Things* (IoT) menghadirkan tantangan baru dalam keamanan jaringan, terutama pada *Low-Power and Lossy Networks* (LLN) yang rentan terhadap serangan *Denial-of-Service* (DoS), seperti serangan UDP flood. Serangan ini mengganggu kinerja jaringan dengan membanjiri target menggunakan paket UDP dalam jumlah besar. Penelitian ini menggunakan metode *rate-based thresholding* untuk mendeteksi serangan UDP flood. Metode ini bekerja dengan memantau jumlah paket yang diterima dalam interval waktu tertentu, membandingkannya dengan ambang batas, dan memberikan peringatan jika ambang batas terlampaui. Simulasi dilakukan menggunakan Contiki Cooja dalam tiga skenario eksperimen dengan topologi yang berbeda, melibatkan 9 hingga 25 node. Hasil penelitian menunjukkan bahwa metode ini mencapai akurasi deteksi serangan rata-rata sebesar 95%. Dalam pengujian konsumsi daya, metode threshold menghasilkan peningkatan konsumsi daya yang kecil, yaitu hanya sebesar 1%-3% dibandingkan dengan kondisi tanpa deteksi, tergantung pada jumlah node yang digunakan.

Kata Kunci: UDP flood, *Low-Power and Lossy Networks* (LLN), *Rate-based thresholding*, Deteksi Serangan, Contiki Cooja

UDP FLOOD ATTACK DETECTION USING RATE BASEDTHRESHOLDING METHOD ON LLN NETWORK

Ghulam Robbani Toha (09011382025121)

Dept. Of Computer System, Faculty of Computer Science, Sriwijaya University

Email : ghulam.toha@gmail.com

ABSTRACT

The advancement of the Internet of Things (IoT) presents new challenges in network security, especially in Low-Power and Lossy Networks (LLN) which are vulnerable to Denial-of-Service (DoS) attacks, such as UDP flood attacks. This attack disrupts network performance by flooding the target with a large number of UDP packets. This study uses the rate-based thresholding method to detect UDP flood attacks. This method works by monitoring the number of packets received in a certain time interval, comparing it to a threshold, and providing an alert if the threshold is exceeded. Simulations were conducted using Contiki Cooja in three experimental scenarios with different topologies, involving 9 to 25 nodes. The results showed that this method achieved an average attack detection accuracy of 95%. In the power consumption test, the threshold method resulted in a small increase in power consumption, which was only 1%-3% compared to the condition without detection, depending on the number of nodes used.

Keywords: *UDP flood, Low-Power and Lossy Networks (LLN), Rate-based thresholding, Attack Detection, Contiki Cooja*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1. Latar Belakang

Internet of Things (IoT) adalah salah satu konsep jaringan yang berkembang paling cepat, menawarkan berbagai aplikasi untuk keuntungan manusia. Kemajuan dalam arsitektur sistem tersemat dan IPv6 terkompresi telah memungkinkan fungsionalitas tumpukan IP dalam perangkat pintar heterogen yang dibatasi sumber daya. [1].

Munculnya teknologi IoT telah memunculkan jenis jaringan khusus baru yang disebut Low-Power and Lossy Network (LLN). LLN memiliki banyak batasan, termasuk tidak hanya perangkat yang dibatasi sumber daya, yang ditandai dengan memori terbatas, daya, dan kemampuan komputasi, tetapi juga tautan komunikasi (yaitu, bandwidth rendah, jangkauan transmisi pendek, dan topologi jaringan yang berubah secara dinamis karena mobile node), yang menyebabkan packet loss tinggi, delay end-to-end rendah, konsumsi power tinggi, dan throughput rendah [2].

Salah satu masalah utama terhadap keamanan jaringan LLN, dan oleh karena itu terhadap operasional perangkat IoT, adalah serangan UDP flood. serangan seperti banjir UDP mudah dipicu dan diperlukan sangat sedikit usaha dari pihak penyerang. UDP Flood serangan melibatkan membanjiri port acak korban mesin dengan mengirimkan paket UDP dalam jumlah besar pesan. Semakin banyak paket yang diterima, mesin korban menjadi tidak responsif terhadap permintaan sah dari mesin lain. Serangan ini dapat dikurangi dengan membatasi laju pesan kesalahan ICMP yang dihasilkan oleh mesin korban. Penerapan pesan kesalahan ICMP yang membatasi laju berlaku sebagai fitur yang melekat pada router modern dan berbagai fitur lainnya sistem operasi tetapi tidak ada di jaringan IoT[3].

Solusi yang saya tawarkan untuk mendeteksi serangan UDP flood pada jaringan LLN adalah dengan menerapkan metode deteksi berbasis ambang batas (threshold rate-based detection). Dalam pendekatan ini, saya mengusulkan penggunaan mekanisme yang mendeteksi serangan dengan cara menghitung jumlah paket yang diterima dalam suatu interval waktu. Jika jumlah paket yang diterima melebihi

ambang batas yang telah ditentukan, maka sistem akan mengidentifikasi adanya serangan UDP flood.[4].

Kekurangan dari metode threshold pada deteksi serangan UDP flood adalah bahwa metode ini mungkin menghasilkan banyak alarm palsu (false positives) jika ada peningkatan lalu lintas yang sah dan tiba-tiba, serta dapat gagal mendeteksi serangan yang berlangsung secara perlahan-lahan (slow-rate attacks) yang berada di bawah ambang batas yang ditetapkan.

Kelebihan dari Metode threshold dalam mendeteksi serangan UDP flood pada jaringan LLN sangat efektif karena memiliki beberapa kelebihan, seperti kemudahan implementasi yang hanya memerlukan penetapan ambang batas tertentu untuk mendeteksi lonjakan trafik mencurigakan, kemampuan untuk mendeteksi serangan dengan cepat ketika volume trafik melebihi threshold yang telah ditentukan, efisiensi penggunaan sumber daya jaringan dan komputasi karena tidak memerlukan analisis kompleks, fleksibilitas dalam penyesuaian threshold sesuai dengan kondisi dan karakteristik jaringan yang berubah, serta kemampuan untuk mendeteksi anomali dalam pola trafik dengan sederhana.

1.2. RUMUSAN MASALAH

Rumusan masalah dalam penelitian ini adalah bagaimana performa metode *rate-based thresholding* dalam mencapai akurasi tinggi dalam mendeteksi serangan *UDP flood* pada jaringan *Low-power and Lossy Network* (LLN), serta bagaimana pengaruhnya terhadap konsumsi daya jaringan tanpa mengorbankan performa power?

1.3. TUJUAN

Berdasarkan penelitian yang dilakukan, adapun tujuan dari penelitian skripsi ini yaitu:

1. Mendeteksi serangan UDP flood yang dapat mengganggu operasional jaringan *Low-power and Lossy Network* (LLN).

2. Menilai performa metode deteksi berbasis ambang batas dalam menjaga keamanan jaringan, sekaligus mempertahankan performa daya, sebagai dasar untuk pengembangan sistem jaringan yang andal dan hemat power.

1.4. MANFAAT

Berdasarkan penelitian yang dilakukan, adapun manfaat dari penelitian skripsi ini, yaitu:

1. Membantu menemukan deteksi serangan UDP flood pada jaringan LLN agar mengidentifikasi potensi ancaman sebelum mereka menyebabkan kerusakan yang lebih besar.
2. Menyediakan data akurasi yang dapat digunakan untuk mengevaluasi performa metode deteksi dalam konteks serangan UDP flood.

1.5. SISTEMATIKA PENULISAN

BAB I PENDAHULUAN

Bab ini berisi mengenai latar belakang penelitian yang dilakukan, tujuan, manfaat, dan sistematika penulisan penelitian

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang penelitian terkait dengan penelitian yang dilakukan, teori yang mendukung, dan rangkuman dari kajian Pustaka

BAB III METODOLOGI PENELITIAN

Bab ini membahas tentang data set yang digunakan untuk penelitian, perangkat yang digunakan, blok diagtam, serta metodologi yang digunakan untuk melakukan penelitian.

BAB IV PEMBAHASAN

Bab ini berisi tentang proses penelitian yang dilakukan serta penjelasan dari penelitian yang dilakukan.

BAB V KESIMPULAN DAN SARAN

Bab ini menjelaskan mengenai kesimpulan penelitian dari yang dilakukan serta saran dari hasil penelitian yang dilakukan.

DAFTAR PUSTAKA

[1] T. A. Al-Amiedy *et al.*, "A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things," *Internet of Things (Netherlands)*, vol. 22, no. September 2022, p. 100741, 2023, doi: 10.1016/j.iot.2023.100741.

[2] K. A. Darabkh, M. Al-Akhras, J. N. Zomot, and M. Atiquzzaman, "RPL routing protocol over IoT: A comprehensive survey, recent advances, insights, bibliometric analysis, recommendations, and future directions," *J. Netw. Comput. Appl.*, vol. 207, no. June, p. 103476, 2022, doi: 10.1016/j.jnca.2022.103476.

[3] Kamaldeep, M. Malik, and M. Dutta, "Contiki-based mitigation of UDP flooding attacks in the Internet of things," *Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA 2017*, vol. 2017-Janua, pp. 1296–1300, 2017, doi: 10.1109/CCAA.2017.8229997.

[4] A. Fuchsberger, "Intrusion detection systems and intrusion prevention systems," *Inf. Secur. Tech. Rep.*, vol. 10, no. 3, pp. 134–139, 2005, doi: 10.1016/j.istr.2005.08.001.

[5] A. Verma and V. Ranga, "Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks," *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 2, pp. 1–25, 2020, doi: 10.1002/ett.3802.

[6] S. Ankam and N. S. Reddy, "A mechanism to detecting flooding attacks in quantum enabled cloud-based lowpower and lossy networks," *Theor. Comput. Sci.*, vol. 941, pp. 29–38, 2023, doi: 10.1016/j.tcs.2022.08.018.

[7] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-Service detection in 6LoWPANbased Internet of Things," *Int. Conf. Wirel. Mob. Comput. Netw. Commun.*, pp. 600–607, 2013, doi: 10.1109/WiMOB.2013.6673419.

[8] A. Tabassum1 and and W. Lebda2, "Security Framework for IoT Devices

against Cyber-Attacks," *Dep. Comput. Sci. Eng. Qatar Univ. Doha, Qatar 1atabassum@qu.edu.qa 2 wadha.lebda@qu.edu.qa AB*, vol. 41, no. 2, pp. 625–644, 2022, doi: 10.32604/csse.2022.020799.

[9] J. David and C. Thomas, "Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic," *Comput. Secur.*, vol. 82, pp. 284–295, 2019, doi: 10.1016/j.cose.2019.01.002.

[10] B. F. L. M. Sousa, N. C. Soeiro, Z. Abdelouahab, W. F. Ribeiro, and D. C. P. Ribeiro, "An intrusion detection system for denial of service attack detection in internet of things," *ACM Int. Conf. Proceeding Ser.*, 2017, doi: 10.1145/3018896.3018962.

[11] A. Bijalwan, M. Wazid, E. S. Pilli, and R. C. Joshi, "Forensics of Random-UDP Flooding Attacks," *J. Networks*, vol. 10, no. 5, pp. 287–293, 2015, doi: 10.4304/jnw.10.5.287-293.

[12] D. Boro, H. Basumatary, T. Goswami, and D. K. Bhattacharyya, "UDP flooding attack detection using information metric measure," *Adv. Intell. Syst. Comput.*, vol. 408, pp. 143–153, 2016, doi: 10.1007/978-981-10-0129-1_16.

[13] Y. T. Tonapa, I. Wahidah, N. Bogi, and A. Karna, "Performance Testing of Routing Protocol for Low Power and Lossy Networks (Rpl) Against Attack Using Cooja Simulator," vol. 7, no. 2, pp. 4093–4101, 2020.

[14] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," *Int. Conf. Wirel. Mob. Comput. Netw. Commun.*, pp. 600–607, 2013, doi: 10.1109/WiMOB.2013.6673419.

[15] E. Garcia Ribera, B. Martinez Alvarez, C. Samuel, P. P. Ioulianou, and V. G. Vassilakis, "An Intrusion Detection System for RPL-Based IoT Networks," *Electron.*, vol. 11, no. 23, 2022, doi: 10.3390/electronics11234041.