PERTAHANAN TERHADAP SERANGAN DENIAL-OF-SERVICE (DOS) DALAM JARINGAN 6LOWPAN DENGAN METODE PENDETEKSIAN BERDASARKAN AMBANG BATAS (*THRESHOLD- BASED DETECTION*)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh
Gelar Sarjana Komputer

OLEH :
MUHAMMAD RIDHO ADE SAPUTRA
09011382025114

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

PERTAHANAN TERHADAP SERANGAN DENIAL-OF-SERVICE (DOS) DALAM JARINGAN 6LOWPAN DENGAN METODE PENDETEKSIAN BERDASARKAN AMBANG BATAS (THRESHOLD- BASED DETECTION)

Sebagai salah satu syarat untuk penyelesaian studi di

Program Studi S1 Sistem Komputer

Oleh:

MUHAMMAD RIDHO ADE SAPUTRA

09011382025114

Pembimbing 1 : **HUDA UBAYA, S.T., M.T.**
NIP. 198106162012121003

Mengetahui
Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T
196612032006041001

AUTHENTICATION PAGE

FINAL TASK

DEFENSE AGAINST DENIAL-OF-SERVICE (DOS) ATTACKS IN 6LOWPAN NETWORKS WITH THRESHOLD-BASED DETECTION METHOD

Submitted to Complete One of the Requirements for Obtaining a Bachelor's Degree in Computer Science

By:

MUHAMMAD RIDHO ADE SAPUTRA

09011382025114

Supervisor 1 : **HUDA UBAYA, S.T., M.T.**
NIP. 198106162012121003

Acknowledge
Head of Computer Systems Department

Dr. Ir. Sukemi, M.T
196612032006041001

HALAMAN PERSETUJUAN

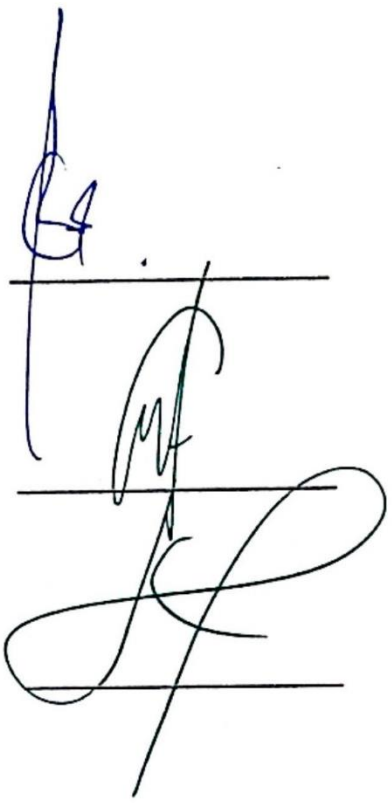
Telah diuji dan lulus pada

Hari : Jum'at

Tanggal : 11 Juli 2025

Tim Penguji :

1. Ketua : Sutarno, M.T.
2. Penguji : Dr. Ahmad Zarkasi, M.T.
3. Pembimbing : Huda Ubaya, M.T.



Mengetahui, 24/7/25

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Muhammad Ridho Ade Saputra

NIM : 09011382025114

Judul : Pertahanan Terhadap Serangan Denial-Of-Service (Dos) Dalam Jaringan 6lowpan Dengan Metode Pendeteksian Berdasarkan Ambang Batas (Threshold- Based Detection)

Hasil pengecekan *Software Turnitin* : 16 %

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya. Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Palembang, 22 Juli 2025

Penulis

Muhammad Ridho Ade Saputra

NIM. 09011382025114

KATA PENGANTAR

Puji dan syukur penulis haturkan atas kehadirat Allah SWT, yang telah memberikan rahmat dan karunia-Nya berupa akal pikiran, ilmu pengetahuan kesehatan dan kekuatan sehingga penulis dapat menyelesaikan penyusunan tugas akhir ini dengan judul **"Pertahanan Terhadap Serangan Denial-Of-Service (Dos) Dalam Jaringan 6lowpan Dengan Metode Pendeteksian Berdasarkan Ambang Batas (Threshold- Based Detection)"** Pada penyusunan tugas akhir ini, tidak lepas dari motivasi, semangat,bimbingan dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur dan terima kasih kepada:

1. Allah Subhanahu Wata'ala yang telah memberikan rahmat dan karunia- Nya kepada penulis dalam penyusunan tugas akhir ini.
2. Orangtua tercinta (Papa Takwanidin dan mama sinda) yang selalu memberikan dukungan baik moral maupun finansial, semangat serta do'a yang tiada hentinya.
3. Keluarga besar penulis yang tersayang. Terima kasih atas semua kebaikan dan dukungan yang diberikan.
4. Bapak Dr. Erwin, M.Si selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Bapak Dr. Ir. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
6. Bapak Huda Ubaya, M.T. selaku PembimbingTugas Akhir penulis di Jurusan Sistem Komputer yang telah meluangkan untuk membimbing dan memberikan motivasi selama kuliah dan pengerjaan Tugas Akhir.
7. Mbak Sari Anhar selaku Admin Jurusan Sistem Komputer yang baik dan ramah dalam membantu administrasi Tugas Akhir.
8. Teman- teman satu kelompok riset yang selalu memberi solusi dan semangat Imam Muttakin dan Muhammad Rizky juliansyah, Sukses untuk kita semua guys!
9. Kakak-kakak tingkat yang menjadi panutan, teman-teman

seperjuangan Jurusan Sistem Komputer Angkatan 2020 terkhusus kelas A, serta semua orang baik yang sempat hadir dalam kehidupan penulis yang tidak dapat penulis cantumkan satu persatu.

10. Civitas Akademika Fakultas Ilmu Komputer Universitas Sriwijaya.
11. Almamater Universitas Sriwijaya.

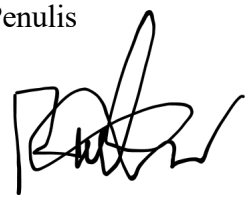
Penulis menyadari bahwa masih ada banyak kekurangan dalam penulisan laporan tugas akhir ini. Mengingat kurangnya pengetahuan dan pengalaman penulis dalam hal ini. Oleh karena itu kritik dan saran yang mendukung sangat penting bagi penulis.

Akhir kata dengan segala keterbatasan, penulis berharap semoga laporan ini menghasilkan sesuatu yang bermanfaat bagi kita semua khususnya bagi mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbangan pikiran dalam peningkatanmatu pembelajaran.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Palembang, 22 Juli 2025

Penulis



Muhammad Ridho Ade Saputra

NIM. 09011382025114

PERTAHANAN TERHADAP SERANGAN DENIAL-OF-SERVICE (DOS) DALAM JARINGAN 6LOWPAN DENGAN METODE PENDETEKSIAN BERDASARKAN AMBANG BATAS (THRESHOLD- BASED DETECTION)

Muhammad Ridho Ade Saputra (09011382025114)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : Muhammadridho12095@gmail.com

ABSTRAK

Pertumbuhan perangkat Internet of Things (IoT) telah mendorong pemanfaatan protokol 6LoWPAN, yang dirancang untuk perangkat dengan keterbatasan sumber daya. Namun, protokol ini memiliki kelemahan terhadap serangan Denial-of-Service (DoS), khususnya UDP Flood, yang dapat menguras energi dan mengganggu komunikasi jaringan. Penelitian ini bertujuan untuk mengembangkan dan mengevaluasi metode threshold-based detection guna mendeteksi serangan DoS secara efisien dalam jaringan 6LoWPAN. Simulasi dilakukan menggunakan Contiki OS dan Cooja Simulator dalam tiga skenario jaringan yang terdiri dari 20, 40, dan 60 node, dengan variasi jumlah node penyerang. Sistem deteksi ini dievaluasi menggunakan parameter True Positive (TP), False Positive (FP), True Negative (TN), dan False Negative (FN). Hasil penelitian menunjukkan bahwa metode ini mampu mencapai tingkat akurasi deteksi di atas 80% pada seluruh skenario, yaitu 80,92%, 81,14%, dan 81,30%, serta tanpa menghasilkan false positive. Selain itu, metode ini juga menunjukkan efisiensi konsumsi daya yang lebih baik dibandingkan kondisi tanpa deteksi. Dengan implementasi yang ringan dan akurat, metode threshold-based detection terbukti efektif untuk meningkatkan ketahanan jaringan 6LoWPAN terhadap serangan DoS.

Kata Kunci : Internet of Things, 6LoWPAN, Denial-of-Service, UDP Flood, threshold-based detection, Contiki, Cooja.

DEFENSE AGAINST DENIAL-OF-SERVICE (DOS) ATTACKS IN 6LOWPAN NETWORKS WITH THRESHOLD-BASED DETECTION METHOD

Muhammad Ridho Ade Saputra (09011382025114)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : Muhammadridho12095@gmail.com

ABSTRAK

The growth of Internet of Things (IoT) devices has driven the adoption of the 6LoWPAN protocol, designed for resource-constrained devices. However, this protocol is vulnerable to Denial-of-Service (DoS) attacks, particularly UDP Flood, which can drain energy and disrupt network communications. This study aims to develop and deploy a threshold-based detection method to efficiently detect DoS attacks in 6LoWPAN networks. Simulations were conducted using Contiki OS and Cooja Simulator in three network scenarios consisting of 20, 40, and 60 nodes, with varying numbers of attacker nodes. The detection system was evaluated using True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN) parameters. The results showed that this method was able to achieve a detection accuracy rate above 80% in all scenarios, namely 80.92%, 81.14%, and 81.30%, without producing false positives. In addition, this method also showed better power consumption efficiency compared to the condition without detection. With lightweight and accurate implementation, the threshold-based detection method is proven to be effective in improving the resilience of 6LoWPAN networks against DoS attacks.

Kata Kunci : Internet of Things, 6LoWPAN, Denial-of-Service, UDP Flood, threshold-based detection, Contiki, Cooja.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Internet of Things (IoT) merupakan salah satu paradigma jaringan yang mengalami perkembangan pesat dalam beberapa tahun terakhir, di mana berbagai perangkat pintar saling terhubung dan mampu bertukar data secara otomatis tanpa campur tangan manusia secara langsung [1]. Internet of things atau yang biasa dikenal dengan IoT merupakan sebuah konsep dimana sebuah benda dapat mentransfer data melalui sebuah jaringan tanpa memerlukan interaksi manusia. Perkembangan pesat ini didorong oleh kemajuan pada arsitektur sistem tertanam dan implementasi IPv6 yang terkompresi, sehingga memungkinkan perangkat IoT yang heterogen dan memiliki sumber daya terbatas dapat menjalankan tumpukan protokol IP secara efisien [2]. Internet of Things menyediakan kemampuan bagi manusia dan komputer untuk belajar dan berkomunikasi dari miliaran hal yang meliputi sensor, actuator layanan dan objek yang terhubung ke internet lainnya. Teknologi utama dalam realisasi sistem IoT adalah middleware, yang biasanya dijelaskan sebagai sistem perangkat lunak yang dirancang untuk menjadi perantara antara perangkat dan aplikasi IoT .Middleware memainkan peran penting karena bertanggung jawab atas sebagian besar kecerdasan dalam IoT, mengintegrasikan data dari perangkat, memungkinkan perangkat untuk berkomunikasi, dan membuat keputusan berdasarkan data yang dikumpulkan (CruzInovasi tersebut mendorong munculnya jaringan khusus yang dikenal sebagai Low-Power and Lossy Network (6LoWPAN), yang mengintegrasikan IPv6 dengan protokol IEEE 802.15.4 untuk mendukung komunikasi pada perangkat dengan keterbatasan daya, memori, serta kemampuan komputasi [3] .

Namun, karakteristik 6LoWPAN yang terdiri dari perangkat dengan sumber daya terbatas dan keterbatasan pada sisi komunikasi seperti bandwidth rendah, jangkauan transmisi pendek, serta topologi yang

dinamis akibat mobilitas node, menyebabkan jaringan ini sangat rentan terhadap berbagai serangan, termasuk serangan Denial of Service (DoS) seperti UDP Flood [3]. Segala kejadian yang mengurangi, mengganggu atau menghilangkan sepenuhnya komunikasi jaringan dikategorikan sebagai serangan DoS. Untuk jaringan informasi apa pun, 'ketersediaan perangkat' merupakan faktor yang paling penting, dan serangan DoS menargetkan 'ketersediaan jaringan' dengan mencegah komunikasi antara perangkat jaringan mengakses layanan yang disediakan. Dengan demikian, serangan DoSdianggap sebagai masalah keamanan yang penting. Serangan ini dapat dimulai dari tempat-tempat terpencil hanya dengan perintah, dikombinasikan dengan alat-alat canggih; penyeran bahkan dapat melakukan serangan DoS terdistribusi, yang efisien dalam melumpuhkan jaringan besar. Agak sulit untuk menemukan serangan DoS sebelum layanan menjadi tidak tersedia[4]. Dampak dari serangan ini antara lain meningkatnya packet loss, delay end-to-end yang rendah, konsumsi daya yang tinggi, serta throughput jaringan yang menurun drastis [5].

Berbagai metode telah dikembangkan untuk mengatasi serangan Denial of Service (DoS) pada jaringan 6LoWPAN, salah satunya adalah pendekatan **Deteksi DDoS Berbasis Ambang Batas di Jaringan Skala Besar** telah melakukan studi mendalam mengenai **deteksi serangan DDoS terdistribusi berbasis ambang batas (*threshold-based detection*) dalam jaringan ISP**. Penelitian ini menggarisbawahi efektivitas metode tersebut dalam mendeteksi serangan skala besar di lingkungan dengan kapasitas jaringan tinggi. Meskipun demikian, penerapan metode ini di jaringan ISP cenderung mengasumsikan ketersediaan sumber daya komputasi dan *bandwidth* yang besar, serta karakteristik lalu lintas yang berbeda dengan lingkungan IoT 6LoWPAN yang memiliki keterbatasan sumber daya [6].

Selanjutnya, Penelitian oleh menunjukkan potensi akurasi tinggi menggunakan *machine learning* untuk deteksi DoS. Namun, pendekatan

ini sering membutuhkan komputasi intensif dan dataset pelatihan yang besar, yang mungkin tidak optimal untuk lingkungan 6LoWPAN dengan sumber daya terbatas[7].

Selain itu, terdapat pendekatan yang berbeda dalam pertahanan DoS, seperti yang diusulkan dalam jurnal **"Cyber Deception Against Battery Drain DoS Attacks in Wireless Sensor Networks Using Signaling Game"** Penelitian ini membahas pertahanan terhadap serangan DoS (khususnya *battery drain attacks*) di **Wireless Sensor Networks (WSN)** dengan menggunakan **Teori Sinyal (*Signaling Game*) dan Teori Permainan (*Game Theory*)** untuk mengembangkan strategi penipuan siber. Meskipun relevan dalam konteks jaringan sensor berdaya rendah, pendekatan ini berfokus pada strategi mitigasi berbasis interaksi penyerang, bukan pada metode deteksi berbasis lalu lintas secara langsung [8].

Melihat kesenjangan dan tantangan di atas, serta mempertimbangkan keterbatasan ekstrem sumber daya pada perangkat 6LoWPAN, oleh karena itu penelitian ini menggunakan metode threshold-based detection. Metode ini dinilai paling cocok dan menjanjikan karena implementasinya yang sederhana dan efisien dari segi penggunaan sumber daya, menjadikannya ideal untuk perangkat IoT berdaya rendah. Meskipun ada tantangan dalam penentuan ambang batas yang adaptif dan akurat untuk mengurangi false positive, potensi efisiensi dan kemampuan respons cepatnya menjadi fokus utama yang akan dioptimalkan dalam penelitian ini.

Oleh karena itu, penelitian ini bertujuan untuk menganalisis, merancang, dan mengevaluasi implementasi threshold-based detection yang optimal untuk deteksi serangan DoS pada jaringan 6LoWPAN, dengan fokus pada penentuan ambang batas yang guna meningkatkan efisiensi dan akurasi deteksi sekaligus mengurangi false positive.

1.2 RUMUSAN MASALAH

Serangan Denial-Of-Service (DoS) merupakan ancaman serius dalam jaringan 6LoWPAN yang dapat mengganggu ketersediaan layanan dan mengakibatkan dampak finansial yang merugikan. Berikut Ini Yang Merupakan Rumusan Masalah dari Penelitian Ini :

1. Bagaimana Menentukan nilai ambang batas dari Parameter-Parameter Yang di Pakai untuk Mendeteksi Serangan DoS dalam konteks IPv6.

2. Bagaimana Cara Mengembangkan Dan Menguji Metode Pendeteksi Ambang Batas Berdasarkan Parameter-Parameter Sebelumnya.

3. Bagaimana Tingkat Keberhasilan Metode Deteksi Ambang Batas Terhadap Serangan Dos Pada Jaringan 6lowpan.

1.3 BATASAN MASALAH

Agar penelitian mengarah pada pemaparan yang diharapkan, maka diperlukan batasan masalah dalam penelitian ini. Adapun batasan masalah tersebut adalah sebagai berikut:

1. Menggunakan 20,40,60 node normal dan node malicious dengan luasan 200x200m.
2. Simulasi menggunakan contiki cooja dengan routing protokol RPL.
3. Menggunakan jenis serangan DoS Flooding Attack.

1.4 TUJUAN

Berikut adalah tujuan dari penulisan Tugas Akhir ini:

1. serangan DoS dan menentukan nilai ambang batasnya.
2. Mengembangkan dan menguji metode deteksi berbasis ambang batas berdasarkan parameter-parameter yang telah ditentukan.
3. Menganalisis tingkat keberhasilan metode deteksi ambang batas dalam mengidentifikasi serangan DoS pada jaringan 6LoWPAN.

1.5 MANFAAT

Berikut adalah manfaat dari penulisan Tugas Akhir ini :

1. Dapat mengetahui parameter-parameter mana yang dominan untuk mendeteksi serangan DoS pada jaringan 6lowpan.
2. Memberikan kontribusi dalam pengembangan metode deteksi serangan DoS berbasis ambang batas yang efektif dan efisien di lingkungan jaringan 6LoWPAN.
3. Memberikan gambaran mengenai tingkat keberhasilan dan efektivitas metode threshold-based detection dalam mengidentifikasi serangan DoS, yang dapat dijadikan acuan dalam pengembangan sistem keamanan jaringan IoT ke depan.

1.6 SISTEMATIKA PENULISAN TENTANG

BAB I PENDAHULUAN

Bab ini berisikan latar belakang, perumusan masalah tujuan, manfaat dan sistematika penulisan.

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 dataset yang digunakan untuk penelitian, perangkat yang digunakan, blok diagram, 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 akan menjelaskan tentang kesimpulan yang didapat dari data penelitian yang telah dilakukan. Dan saran yang diharapkan dapat membuat penelitian ini dikembangkan lebih baik.

DAFTAR PUSTAKA

[1] D. Conzon, P. Brizzi, P. Kasinathan, C. Pastrone, F. Pramudianto, and P. Cultrona, "Industrial application development exploiting IoT vision and model driven programming," *2015 18th Int. Conf. Intell. Next Gener. Networks, ICIN 2015*, no. March, pp. 168–175, 2015, doi: 10.1109/ICIN.2015.7073828.

[2] D. Chasaki and C. Mansour, "Security challenges in the internet of things," *Int. J. Space-Based Situated Comput.*, vol. 5, no. 3, p. 141, 2015, doi: 10.1504/ijssc.2015.070945.

[3] H. Kopetz, "Internet of Things Strategic Research Roadmap," no. December 2014, pp. 307–323, 2009, [Online]. Available: \

[4] A. Le, J. Loo, K. K. Chai, and M. Aiash, "A specification-based IDS for detecting attacks on RPL-based network topology," *Inf.*, vol. 7, no. 2, 2016, doi: 10.3390/info7020025.

[5] R. Riaz, K. H. Kim, and H. F. Ahmed, "Security analysis survey and framework design for IP connected LoWPANs," *Proc. - 2009 Int. Symp. Auton. Decentralized Syst. ISADS 2009*, no. October 2020, pp. 29–34, 2009, doi: 10.1109/ISADS.2009.5207373.

[6] I. Sadek, J. Codjo, S. U. Rehman, and B. Abdulrazak, "Security and privacy in the internet of things healthcare systems: Toward a robust solution in real-life deployment," *Comput. Methods Programs Biomed. Updat.*, vol. 2, no. July, p. 100071, 2022, doi: 10.1016/j.cmpbup.2022.100071.

[7] A. Abduvaliyev, S. Lee, and Y. K. Lee, “Energy efficient hybrid intrusion detection system for wireless sensor networks,” *ICEIE 2010 - 2010 Int. Conf. Electron. Inf. Eng. Proc.*, vol. 2, no. Iceie, pp. 25–29, 2010, doi: 10.1109/ICEIE.2010.5559708.

[8] S. Karanbir, D. Kanwalvir Singh, and B. Bharat, “Threshold-based distributed. DDoS attack detection in ISP networks,” *Turkish J. Electr. Eng. Comput. Sci.*, vol. 26, no. 4, pp. 1796–1811, 2018, doi: 10.3906/elk-1712-3.

[9] 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.*, no. October, pp. 600–607, 2013, doi: 10.1109/WiMOB.2013.6673419.

[10] R. Achmad, E. V. Manullang, and E. R. Sanmas, “Rancang Bangun Aplikasi Deteksi Dan Penanganan Serangan Ddos Dan Port Scanning Memanfaatkan Snort Pada Jaringan Komputer,” *J. Teknol. Inf.*, vol. 8, no. 1, pp. 2–11, 2020.