DETEKSI SERANGAN DENIAL OF SERVICE (DOS) DALAM JARINGAN 6LOWPAN DENGAN METODE BERDASARKAN BASIS KEPERCAYAAN (TRUST BASED DETECTION)

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh Gelar Sarjana Komputer

DISUSUN OLEH:

ARIFAN LONCIMITA

09011382025129

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

DETEKSI SERANGAN DENIAL-OF-SERVICE (DOS) DALAM JARINGAN 6LOWPAN DENGAN METODE BERDASARKAN BASIS KEPERCAYAAN(TRUST BASED DETECTION)

Sebagai Salah Satu Syarat Untuk Penyelesaian Studi Di

Program Studi Sistem Komputer (S1)

Oleh:

ARIFAN LONCIMITA

09011382025129

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

Mengatahui

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M. T.

NIP. 196612032006041001

AUTHENTICATION PAGE

FINAL TASK

DETECTION AGAINST DENIAL-OF-SERVICE (DOS) ATTACKS IN 6LOWPAN NETWORK WITH TRUST BASED DETECTION METHOD

Submitted to Complete One of the Requirements for Obtaining a Bachelor's

Degree in Computer Science

By:

ARIFAN LONCIMITA

09011382025129

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 : 26 September 2025

Tim Penguji :

1. Ketua : Imam Saladin B. Azhar, S.Kom M.MSi. _____

2. Penguji : Ahmad Fali Oklilas, M.T. _____

3. Pembimbing : Huda Ubaya, M.T. _____

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini :

Nama : Arifan Loncimita

NIM : 09011382025129

Judul : DETEKSI SERANGAN DENIAL OF SERVICE (DOS) DALAM JARINGAN 6LOWPAN DENGAN METODE BERDASARKAN BASIS KEPERCAYAAN (TRUST BASED DETECTION)

Hasil pengecekan *Software Turnitin* : 11 %

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, September 2025

Penulis

Arifan Loncimita

NIM. 09011382025129

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 Denial-Of-Service (Dos) Dalam Jaringan 6lowpan Dengan Metode Berdasarkan Basis Kepercayaan(Trust Based Detection)".**

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 Ridwan AW dan Ibu Zubaidah Mursid 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. H. 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 Prof. Dr. Ir. Siti Nurmaini, M.T selaku Dosen Pembimbing Akadamik Jurusan Sistem Komputer penulis saat ini.

7. Admin jurusan Sistem Komputer yang telah berjasa dalam membantu permasalahan administrasi penulis.
8. Teman-teman dari Sistem Komputer Angkatan 2020 yang telah memberikan banyak support dan bantuan selama penulis menjalani masa perkuliahan hingga akhir.
9. Semua pihak yang terlibat yang telah turut ikut membantu, baik itu dalam memberikan masukan dan ide, kritik maupun juga memberikan semangat kepada penulis yang mana tidak dapat disebutkan satu persatu.

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, September 2025

Penulis

Arifan Loncimita

NIM. 09011382025129

DETEKSI SERANGAN DENIAL OF SERVICE (DOS) DALAM JARINGAN 6LOWPAN DENGAN METODE BERDASARKAN BASIS KEPERCAYAAN (TRUST BASED DETECTION)

Arifan Loncimita (0901138202519)

Jurusan Sistem Komputer,Fakultas Ilmu Komputer ,Universitas Sriwijaya

Email : arifannn15@gmail.com

ABSTRAK

Jaringan *Internet of Things* (IoT), khususnya 6LoWPAN yang mengadopsi protokol routing RPL, sangat rentan terhadap ancaman keamanan seperti serangan *Denial-of-Service* (DoS). Serangan UDP *Flooding* secara spesifik dapat mengganggu ketersediaan layanan dan menguras sumber daya terbatas node. Penelitian ini mengusulkan dan mengevaluasi kinerja metode *Trust-based* detection untuk mendeteksi serangan DoS dalam jaringan 6LoWPAN. Metode ini menilai tingkat kepercayaan node melalui dua parameter utama: *Direct Trust* (DT), yang dihitung dari rasio paket valid, dan *Indirect Trust* (IT), yang didapatkan dari skor reputasi node tetangga. Simulasi Contiki Cooja menunjukkan bahwa node malicious terdeteksi dengan jelas karena menghasilkan jumlah paket yang sangat tinggi dan memiliki nilai *Direct Trust* yang sangat rendah (0.73%–0.97%), serta *Indirect Trust* yang mencerminkan ketidakpercayaan tinggi (18%–20%). Selain itu, implementasi mekanisme deteksi *Trust-based* terbukti efisien dengan konsumsi daya yang stabil atau sedikit hemat energi dibandingkan kondisi serangan tanpa deteksi, memastikan kelayakan metode ini untuk jaringan 6LoWPAN yang terbatas sumber daya.

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

DETECTION AGAINST DENIAL-OF-SERVICE (DOS) ATTACKS IN 6LOWPAN NETWORK WITH TRUST BASED DETECTION METHOD

Arifan Loncimita (0901138202519)

Department of Computer Systems, Faculty of Computer Science, Sriwijaya University

Email : arifannn15@gmail.com

ABSTRACT

Internet Of Things (Iot) Networks, Especially 6lowpan Utilizing The RPL Routing Protocol, Are Highly Susceptible To Security Threats Such As Denial-Of-Service (Dos) Attacks. Specifically, The UDP Flooding Attack Can Disrupt Service Availability And Deplete The Limited Resources Of Network *Nodes*. This Research Proposes And Evaluates The Performance Of The Trust-Based Detection Method For Detecting Dos Attacks In 6lowpan Networks. This Method Assesses The *Node's* Trust Level Through Two Main Parameters: Direct Trust (DT), Calculated From The Ratio Of Valid Packets, And Indirect Trust (IT), Derived From The Reputation Score Of Neighboring *Nodes*. Contiki Cooja Simulations Clearly Showed That *Malicious Nodes* Were Detected By Generating An Extremely High Number Of Packets And Having Very Low DT Values (0.73%–0.97%), While IT Reflected High Distrust (18%–20%). Furthermore, The Implementation Of The Trust-Based Mechanism Proved Energy-Efficient, Showing Stable Or Slightly Reduced Power Consumption Compared To An Undetected Attack Scenario, Confirming Its Feasibility For Resource-Constrained 6lowpan Networks.

Keywords : Internet of Things, 6LoWPAN, Denial-of-Service,UDP Flood, Trust-based detection, Contiki, Cooja.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Konsep "Internet of Things (IoT)" mengacu pada jaringan perangkat fisik yang terhubung ke internet dan memiliki kemampuan untuk berkomunikasi satu sama lain. Perangkat-perangkat ini, yang mencakup sensor, kendaraan, perangkat rumah tangga, dan mesin industri, dapat mengumpulkan dan berbagi data secara otomatis tanpa memerlukan intervensi manusia. Perangkat IoT dapat "berpikir" dan "berinteraksi" dengan lingkungan mereka, yang menghasilkan ekosistem yang cerdas dan terintegrasi[1].

International Data Corporation (IDC) memperkirakan bahwa pada tahun 2025 akan ada 55,7 miliar perangkat Internet of Things (IoT) atau "benda" yang

terhubung ke Internet, yang akan menghasilkan sekitar 80 miliar ZettaBytes (ZB) data di seluruh dunia[2]. Akibatnya, keamanan lapisan jaringan IoT telah menjadi salah satu topik yang paling banyak diteliti dalam beberapa dekade terakhir, karena, tidak seperti jaringan tradisional, IoT memungkinkan interkonektivitas yang tersebar, yang membuatnya rentan terhadap berbagai ancaman keamanan dan menimbulkan banyak masalah keamanan[3].

Dalam era transformasi digital yang terus berkembang, jaringan Internet of Things (IoT) menjadi sangat penting untuk menghubungkan perangkat dan menyediakan layanan. Namun, semakin majunya teknologi juga membawa ancaman baru, seperti serangan Denial-of-Service (DoS), yang dapat mengganggu ketersediaan sumber daya jaringan. Serangan ini bisa merugikan pengguna dan penyedia layanan. Oleh karena itu, melindungi jaringan IoT dari serangan DoS menjadi sangat penting untuk menjaga kelancaran operasional dan kehandalan layanan.

DoS sering dipicu dengan mengirimkan sejumlah besar paket dalam jangka waktu yang lama atau dengan mengirimkan sejumlah besar paket pada waktu yang sama dan mencekik server. Ada banyak alat di Internet dengan skrip PHP dan Perl, jadi tidak sulit untuk mengimplementasikan serangan ini. Banyak PC zombie berpartisipasi dalam serangan ini dan melakukan serangan DoS. Individu atau kelompok yang tidak bermoral dapat menggunakan Internet untuk memblokir atau menghapus situs web, mengalihkan router, dan menolak akses ke orang lain[4].

studi mengungkapkan bahwa keamanan jaringan merupakan elemen kunci dalam mendukung konektivitas IoT, termasuk pada jaringan 5G yang menghadapi tantangan serius dari serangan siber,sehingga memerlukan pendekatan mitigasi yang sistematis melalui enkripsi dan autentikasi

Menurut berbagai studi, metode deteksi serangan berbasis kepercayaan (trust-based detection) telah terbukti menjadi pendekatan yang efektif dalam

mengatasi ancaman DoS, khususnya pada jaringan 6LoWPAN. Pendekatan ini mengandalkan nilai kepercayaan antar node dalam jaringan untuk mengenali perilaku tidak wajar yang dapat mengindikasikan aktivitas serangan. Dengan mengintegrasikan mekanisme kepercayaan, proses pendeteksian menjadi lebih efisien serta mampu mengurangi tekanan terhadap keterbatasan sumber daya perangkat jaringan sensor.

Melalui penelitian ini, diharapkan dapat memberikan kontribusi yang berharga dalam pemahaman tentang pertahanan terhadap serangan DoS dalam jaringan 6LoWPAN serta menghasilkan metode pendeteksian yang dapat meningkatkan keamanan dan ketersediaan layanan dalam lingkungan ini.

1.2 Rumusan Masalah

Rumusan masalah dari penelitian Tugas Akhir yang dilakukan:

1. Bagaimana mendeteksi serangan Denial of Service (Dos) pada jaringan 6LoWPAN dengan pendeteksian berdasarkan kepercayaan?
2. Bagaimana kinerja metode pendeteksian berdasarkan kepercayaan untuk mencegah adanya serangan Denial of Service (Dos) pada jaringan 6LoWPAN agar paket tetap sampai pada Node tujuan yang sebenarnya?
3. Bagaimana pengaruh penerapan metode pendeteksian berdasarkan kepercayaan dalam serangan Denial of Service (DoS) terhadap perbedaan konsumsi daya dan efisiensi pada jaringan 6LoWPAN??

1.3 Batasan Masalah

Berdasarkan pemaparan latar belakang, maka dapat diuraikan perumusan masalahyang terdiri atas :

1. Penelitian ini hanya akan fokus pada deteksi serangan Denial of Service (DoS) pada jaringan 6LoWPAN.

2. Simulasi menggunakan Contiki Cooja dengan routing protokol jaringan RPL
3. Menggunakan 20,40,60 node normal dan node malicious dengan luasan 200x200m

1.4 Tujuan

Tujuan dari penulisan Tugas Akhir ini:

1. Mengembangkan metode deteksi kepercayaan yang efektif untuk mendeteksi serangan Denial of Service pada jaringan 6LoWPAN.
2. Menilai kinerja metode deteksi serangan Denial of Service dalam jaringan 6loWPAN dengan menggunakan metode berdasarkan basis kepercayaan
3. Menganalisis pengaruh metode berdasarkan kepercayaan terhadap konsumsi daya dan efisiensi energi pada skenario node jaringan 6WOLPAN.

1.5 Manfaat

Manfaat dari penulisan Tugas Akhir ini :

1. Meningkatkan keandalan jaringan 6LoWPAN dengan memberikan proses deteksi yang efektif terhadap serangan Denial of Service.
2. Menjadi referensi bagi peneliti lain dalam mengembangkan metode deteksi serangan Denial of Service dalam jaringan 6loWPAN.
3. Meningkatkan keamanan pada jaringan 6LoWPAN dengan mengidentifikasi dan mencegah serangan Denial of Service (Dos).

1.6 Sistematika Penulisan

Sistematika yang digunakan dalam penulisan tugas akhir ini adalah :

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

Bab ini berisi kesimpulan dari hasil dan analisa dari keseluruhan penelitian yang dilakukan.

Daftar Pustaka

[1] S. Karmakar, J. Sengupta, and S. Das Bit, "LEADER: Low Overhead Rank Attack Detection for Securing RPL based IoT," in *2021 International Conference on COMmunication Systems and NETworkS, COMSNETS 2021*, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 429–437. doi: 10.1109/COMSNETS51098.2021.9352937.

[2] S. S. Ambarkar and N. Shekokar, "An efficient authentication technique to protect iot networks from impact of rpl attacks," *International Journal of Engineering Trends and Technology*, vol. 69, no. 10, pp. 137–145, Oct. 2021, doi: 10.14445/22315381/IJETT-V69I10P217.

[3] M. A. Boudouaia, A. Abouaissa, A. Benayache, and P. Lorenz, "Divide and conquer-based attack against RPL routing protocol," in *Proceedings - IEEE Global Communications Conference, GLOBECOM*, 2020. doi: 10.1109/GLOBECOM42002.2020.9322275.

[4] P. Thulasiraman and Y. Wang, "A Lightweight Trust-Based Security Architecture for RPL in Mobile IoT Networks."

[5] S. Deshmukh-Bhosale and S. S. Sonavane, "Design of intrusion detection system for dos attack in 6lowpan and RPL based iot network," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 11, pp. 3840–3844, Sep. 2019, doi: 10.35940/ijitee.K2288.0981119.

[6] S. Y. Hashemi and F. Shams Aliee, “Dynamic and comprehensive trust model for IoT and its integration into RPL,” *Journal of Supercomputing*, vol. 75, no. 7, pp. 3555–3584, Jul. 2019, doi: 10.1007/s11227-018-2700-3.

[7] D. Airehrour, J. A. Gutierrez, and S. K. Ray, “SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things,” *Future Generation Computer Systems*, vol. 93, pp. 860–876, Apr. 2019, doi: 10.1016/j.future.2018.03.021.

[8] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, “Trust-aware and cooperative routing protocol for IoT security,” *Journal of Information Security and Applications*, vol. 52, Jun. 2020, doi: 10.1016/j.jisa.2020.102467.

[9] K. Prathapchandran and T. Janani, “A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest – RFTRUST,” *Computer Networks*, vol. 198, Oct. 2021, doi: 10.1016/j.comnet.2021.108413.

[10] T. ul Hassan, M. Asim, T. Baker, J. Hassan, and N. Tariq, “CTrust-RPL: A control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks-based Internet of Things applications,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 3, Mar. 2021, doi: 10.1002/ett.4224.

[11] K. Prathapchandran and T. Janani, “A Trust-Based Security Model to Detect Misbehaving Nodes in Internet of Things (IoT) Environment using Logistic Regression,” in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Jul. 2021. doi: 10.1088/1742-6596/1850/1/012031.

[12] Z. A. Khan, P. Herrmann, J. Ullrich, and A. G. Voyiatzis, “A trust-based resilient routing mechanism for the internet of things,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Aug. 2017. doi: 10.1145/3098954.3098963.

[13] S. M. Muzammal, R. K. Murugesan, N. Z. Jhanjhi, M. Humayun, A. O. Ibrahim, and A. Abdelmaboud, “A Trust-Based Model for Secure Routing against RPL Attacks in Internet of Things,” *Sensors*, vol. 22, no. 18, Sep. 2022, doi: 10.3390/s22187052.