DETEKSI SERANGAN BLACKHOLE PADA JARINGAN 6LOWPAN MENGGUNAKAN METODE PENDETEKSIAN BERDASARKAN AMBANG BATAS

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat MemperolehGelar Sarjana Komputer

OLEH :

MUHAMMAD RIZKY JULIANSYAH

09011382025146

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2025

HALAMAN PENGESAHAN

SKRIPSI

DETEKSI SERANGAN BLACKHOLE PADA JARINGAN 6LOWPAN MENGGUNAKAN METODE PENDETEKSIAN BERDASARKAN AMBANG BATAS

Sebagai salah satu syarat untuk penyelesaian studi di
Program Studi S1 Sistem Komputer

Oleh:
MUHAMMAD RIZKY JULIANSYAH
09011382025146

Pembimbing 1 : Huda Ubaya. M.T.
NIP. 198106162012121003

Mengetahui, 09 Juli 2025
Ketua Jurusan Sistem Komputer

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

AUTHENTICATION PAGE

BLACKHOLE ATTACK DETECTION ON 6LOWPAN NETWORK USING THRESHOLD BASED DETECTION METHOD

SKRIPSI

Submitted To Complete One Of The Requirements For Obtaining
A Bachelor's Degree In Computer Science

By:
Muhammad Rizky Juliansyah
09011382025146

Mentor 1 : **Huda Ubaya. M.T.**
NIP. 198106162012121003

Acknowledge, 09 July 2025
Head Of Computer Sciene Departement

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

LEMBAR PERSETUJUAN

Telah diuji dan lulus pada :

Hari : **Jumat**

Tanggal : **23 Mei 2025**

Tim Penguji :

1. **Ketua** : **Dr. Ir. Ahmad Heryanto, M.T.**

2. **Penguji** : **Dr. Ahmad Zarkasi, M.T.**

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

Mengetahui, 9/7/25

Ketua Jurusan Sistem Komputer

KEMENTERIAN PENDIDIKAN TINGGI, SAINS DAN TEKNOLOGI UNIVERSITAS SRIWIJAYA JURUSAN SISTEM KOMPUTER

Dr. Ir. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama : Muhammad Rizky Juliansyah

NIM : 09011382025146

Judul : DETEKSI SERANGAN BLACKHOLE PADA JARINGAN 6LOWPAN MENGGUNAKAN METODE PENDETEKSIAN BERDASARKAN AMBANG BATAS.

Hasil Pengecekan software iThenticated Turnitin : 8%

Menyatakan Bahwa Laporan Tugas Akhir Saya Merupakan Hasil Karya Sendiri Dan Bukan Hasil Pengjiplakan Atau Plagiat. Ditemukan Unsur Penjiplakan Atau Plagiat Dalam Laporan Tugas Akhir Ini, Maka Saya Menerima Sanksi Akademik Dari Universitas Sriwijaya.

Demikian, Pernyataan Ini Saya Buat Dalam Keadaan Sadar Dan Tanpa Paksaan Dari Siapapun.

Palembang, 9 Juli 2025
Yang Menyatakan

Muhammad Rizky Juliansyah
NIM. 09011382025146

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 **"Deteksi Serangan Blackhole Pada Jaringan 6LoWPAN Menggunakan Metode Pendeteksian Berdasarkan Ambang Batas"** 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 Widodo dan Mama Hilda) 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 Ridho Ade Saputra, 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, Juli 2025
Penulis

Muhammad Rizky Juliansyah
NIM. 09011382025146

DETEKSI SERANGAN BLACKHOLE PADA JARINGAN 6LOWPAN MENGGUNAKAN METODE PENDETEKSIAN BERDASARKAN AMBANG BATAS

Muhammad Rizky Juliansyah (09011382025146)

Jurusan sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email: member.gc007@gmail.com

ABSTRAK

Deteksi Serangan Blackhole Pada Jaringan 6LoWPAN Masih Memiliki Beberapa Kekurangan, Seperti Akurasi Deteksi Yang Terbatas Karena Hanya Bergantung Pada Satu Parameter, Overhead Komunikasi Yang Tinggi Akibat Penggunaan Enkripsi Atau IDS, Serta Kurangnya Adaptasi Terhadap Karakteristik Jaringan IOT Yang Heterogen. Metode Ambang Batas Menawarkan Solusi Yang Lebih Efisien Dengan Menggabungkan Analisis Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR), Dan Delay Secara Bersamaan, Sehingga Mampu Meningkatkan Akurasi Deteksi, Mengurangi Konsumsi Daya Serta Lebih Adaptif Terhadap Dinamika Jaringan 6LoWPAN. Kata Kunci : Blackhole, 6LoWPAN, Metode Ambang Batas.

BLACKHOLE ATTACK DETECTION ON 6LOWPAN NETWORK USING THRESHOLD BASED DETECTION METHOD

Muhammad Rizky Juliansyah (09011382025146)

Departement of computer systems, faculty of computer science sriwijaya university

Email: member.gc007@gmail.com

ABSTRACT

Blackhole Attack Detection on 6LoWPAN Networks Still Has Several Disadvantages, Such as Limited Detection Accuracy Because It Only Depends on One Parameter, High Communication Overhead Due to the Use of Encryption or IDS, and Lack of Adaptation to Heterogeneous IoT Network Characteristics. The Threshold Method Offers a More Efficient Solution by Combining Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR), and Delay Analysis Simultaneously, So That It Can Improve Detection Accuracy, Reduce Power Consumption and Be More Adaptive to 6LoWPAN Network Dynamics. Keywords: Blackhole, 6LoWPAN, Threshold Method.

DAFTAR ISI

Halaman

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi jaringan nirkabel telah membawa dampak signifikan dalam berbagai bidang, salah satunya adalah *Wireless Sensor Network* (WSN). WSN merupakan jaringan yang terdiri dari sejumlah sensor nirkabel yang berfungsi untuk mengumpulkan dan mentransmisikan data ke sistem pusat. Jaringan ini banyak digunakan dalam berbagai aplikasi seperti pemantauan lingkungan, industri, kesehatan, dan *Internet of Things* (IoT). Namun, keterbatasan sumber daya seperti daya baterai, kapasitas komputasi, dan *bandwidth* menjadi tantangan utama dalam implementasi WSN, sehingga diperlukan protokol komunikasi yang efisien untuk memastikan keandalan jaringan.

Salah satu solusi yang digunakan dalam WSN adalah 6LoWPAN (IPv6 *over Low-Power Wireless Personal Area Networks*). 6LoWPAN merupakan standar jaringan yang memungkinkan perangkat sensor dengan daya rendah untuk menggunakan IPv6 sebagai protokol komunikasi. Dengan teknologi ini, perangkat IoT dapat terhubung langsung ke jaringan internet, mendukung komunikasi skala besar, serta memungkinkan penggunaan alamat unik untuk setiap perangkat. Keunggulan 6LoWPAN dalam mendukung komunikasi efisien membuatnya menjadi pilihan utama dalam implementasi jaringan berbasis IoT [1].

Serangan yang dilakukan oleh node berbahaya ini (malicious node) sering disebut sebagai *Black Hole Attack*. Dampak dari *Black Hole Attack* terhadap jaringan sensor nirkabel adalah memungkinkan tujuan pengiriman paket yang dikirimkan oleh node sumber diakuisisi oleh *malicious node*. *Black hole* ini akan mengatasnamakan dirinya sebagai node tujuan. Kemudian melakukan drop pada paket atau meneruskan ke *black hole* lain yang paket tidak akan pernah sampai ke node tujuan. *Black hole* akan melakukan pengiriman pesan *Route Reply* (RREP) kepada *node* sumber yang telah diakuisisi oleh *Black Hole* [2]. Pada kondisi ini, *node* sumber tidak dapat membedakan antara node asli dan *Malicious node.*

Penelitian sebelumnya tentang deteksi serangan *blackhole* pada jaringan

6LoWPAN masih memiliki beberapa kekurangan, seperti akurasi deteksi yang terbatas karena hanya bergantung pada satu parameter, overhead komunikasi yang tinggi akibat penggunaan enkripsi atau IDS, serta kurangnya adaptasi terhadap karakteristik jaringan IoT yang heterogen [3]. Metode ambang batas menawarkan solusi yang lebih efisien dengan menggabungkan analisis *Packet Delivery Ratio* (PDR), *Packet Loss Ratio* (PLR), dan delay secara bersamaan, sehingga mampu meningkatkan akurasi deteksi, mengurangi konsumsi daya, serta lebih adaptif terhadap dinamika jaringan 6LoWPAN

Untuk mengatasi serangan blackhole penelitian ini menggunakan nilai ambang batas yang digunakan dalam menentukan dan mengidentifikasi serangan *blackhole* yang ada pada 6LoWPAN [4]. Ambang batas dapat dugunakan untuk melihat nilai ambang tertentu yang digunakan untuk membedakan perilaku normal dan perilaku serangan *blackhole* seperti ambang batas dapat berupa nilai ambang daya diterima atau karakteristik lain yang digunakan sebagai dasar dalam proses deteksi. Parameter ambang batas yang digunakan adalah daya terima (*received signal strength*) dari paket data yang diterima oleh perangkat [5].

Berdasarkan penjelasan diatas, penelitian ini akan membahas mengenai Blackhole dengan judul **"Deteksi Serangan Blackhole Pada Jaringan 6LoWPAN Menggunakan Metode Pendeteksian Berdasarkan Ambang Batas".** Diharapkan penelitian ini akan bermanfaat untuk penelitian selanjutnya.

1.2 Rumusan Masalah

Berikut ini merupakan rumusan masalah dari penelitian Tugas Akhir yang dilakukan:

1. Menganalisis serangan *Blackhole* pada jaringan 6LoWPAN dengan pendeteksian berdasarkan Ambang Batas menggunakan Contiki cooja
2. Menganalisis rasio kehilangan paket pada jaringan 6LoWPAN menggunakan metode ambang batas seperti rasio paket *loss,* dan rate pengiriman ulang paket
3. Menganalisis delay yang terjadi ketika melakukan pengiriman paket antar node untuk peningkatan latensi dan konsumsi energi

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. Analisis dampak serangan berdasarkan ambang daya sinyal dan konsumsi daya tiap *node* terhadap kinerja jaringan.
2. Evaluasi performa jaringan dengan variasi jumlah node (50-200), *malicious node* (5-20%), dan ukuran data (64B-512B).
3. Deteksi serangan Blackhole pada jaringan 6LoWPAN menggunakan metode ambang batas daya sinyal (-85 dBm) dan analisis rasio kehilangan pake

1.4 Tujuan

Berikut adalah tujuan dari penulisan Tugas Akhir ini:

1. Mengembangkan model simulasi WSN yang efektif untuk mendeteksi serangan *Blackhole* pada jaringan 6LoWPAN.
2. Menganalisis packet loss dan rate pengiriman ulang paket yang terjadi pada jaringan 6LoWPAN.
3. Menganalisis efek serangan pada peningkatan latensi dan konsumsi energi yang terjadi pada jaringan 6LoWPAN.

1.5 Manfaat

Berikut adalah manfaat dari penulisan Tugas Akhir ini :

1. Meningkatkan keandalan jaringan 6LoWPAN dengan memberikan proses deteksi yang efektif terhadap serangan *Blackhole*.
2. Dapat mengetahui hasil dari kehilangan paket dan persentase nilai ambang batas yang baik dari jaringan 6LoWPAN
3. Dapat mengidentifikasi serangan *Blackhole* yang datang jika terjadi kenaikan *delay* yang signifikan

1.6 Sistematika Penulisan

Berikut ini merupakan sistematika yang digunakan dalam penulisan tugas akhir agar mendeskripsikan bab-bab yang terdapat dalam tugas akhir yang dilakukan:

BAB I PENDAHULUAN

Bab ini akan menjelaskan tentang latar belakang masalah yang terjadi pada jaringan 6LowPAN Ketika terjadi serangan *blackhole*, tujuan dan manfaat, perumusan masalah, batasan masalah, metodologi penelitian, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang penelitian terkait mengenai *Blackhole attack* , 6LowPAN , PDR, PLR, dan delay dengan penelitian yang dilakukan, teori yang mendukung, dan rangkuman dari kajian Pustaka.

BAB III METODELOGI

Bab ini membahas tentang metode yang digunakan untuk penelitian, perangkat yang digunakan, blok diagram, serta metodologi yang digunakan untuk melakukan penelitian mengenai jaringan 6LowPAN.

BAB IV ANALISA DAN PEMBAHASAN

Bab ini akan menganalisa dan menjelaskan tentang hasil dari pengolahan data yang telah dilakukan, dari hasil tersebut akan dilakukan analisa mengenai dampak yang terjadi pada jaringan 6LowPAN ketika terjadi serangan *blackhole* menggunakan metode ambang batas.

BAB V KESIMPULAN

Bab ini akan menjelaskan tentang kesimpulan yang didapat dari data penelitian yang telah dilakukan.mengenai dampak dari serangan *blackhole* pada jaringan 6LowPAN.

DAFTAR PUSTAKA

[1] F. A. ROSYADA, "Implementasi Pendeteksian dan Pencegahan Serangan Black Hole dengan Memanfaatkan Hop Count dan Neighbor Information pada Jaringan MANET," 2017.

[2] P. Studi, T. Informatika, J. T. Informatika, F. I. Komputer, and U. Brawijaya, *PENDETEKSIAN SERANGAN BLACKHOLE MENGGUNAKAN ENCOUNTER RECORD TERHADAP PROTOKOL ROUTING MULTI-COPY PADA DELAY TOLERANT NETWORK (DTN)*. 2019.

[3] "Data driven intrusion detection for 6LoWPAN based IoT systems."

[4] A. Apriyanti, V. Suryani, and A. A. Wardana, "Penerapan Metode Anomaly Based Detection Untuk Mendeteksi Serangan Black Hole Pada Topologi Mesh Di Lora," *e-Proceeding Eng.*, vol. 7, no. 2, p. 8167, 2020.

[5] A. . A. K. Faruq, S. Wahyuningsih, H. Ahmad, and I. Indarto, "Analisis Kejadian Banjir Menggunakan Metode Ambang Batas (Threshold Level Method)," *Berk. Ilm. Teknol. Pertan.*, vol. 1, no. 1, pp. 1–6, 2015.

[6] N. Khanna and M. Sachdeva, "A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs," *Comput. Sci. Rev.*, vol. 32, pp. 24–44, 2019, doi: 10.1016/j.cosrev.2019.03.001.

[7] "Effectiveness of HT-assisted sinkhole and blackhole denial of service attacks targeting mesh networks-on-chip."

[8] M. Amin, "InfoTekJar :Jurnal Nasional Informatika dan Teknologi Jaringan Sistem Cerdas Kontrol Kran Air Menggunakan Mikrokontroler Arduino dan Sensor Ultrasonic," vol. 4, no. 2, 2020, doi: 10.30743/infotekjar.v4i2.2386.

[9] D. K. Sharma, S. K. Dhurandher, S. Kumaram, K. Datta Gupta, and P. K. Sharma, "Mitigation of black hole attacks in 6LoWPAN RPL-based Wireless sensor network for cyber physical systems," *Comput. Commun.*, vol. 189, no. April, pp. 182–192, 2022, doi: 10.1016/j.comcom.2022.04.003.

[10] H. B. Patel and D. C. Jinwala, "Trust and Strainer Based Approach for Mitigating Blackhole Attack in 6LoWPAN: A Hybrid Approach," *IAENG Int. J. Comput. Sci.*, vol. 48, no. 4, 2021.

[11] X. Wang, Z. Dou, D. Wang, and Q. Sun, "Mobility management for 6LoWPAN WSN," *Comput. Networks*, vol. 131, pp. 110–128, 2018, doi: 10.1016/j.comnet.2017.12.005.

[12] T. J. Nagalakshmi, A. K. Gnanasekar, G. Ramkumar, and A. Sabarivani, “Machine learning models to detect the blackhole attack in wireless adhoc network,” *Mater. Today Proc.*, vol. 47, pp. 235–239, 2021, doi: 10.1016/j.matpr.2021.04.129.

[13] B. Prabhakar Reddy, B. Bhaskar Reddy, and B. Dhananjaya, “The AODV routing protocol with built-in security to counter blackhole attack in MANET,” *Mater. Today Proc.*, vol. 50, pp. 1152–1158, 2021, doi: 10.1016/j.matpr.2021.08.039.

[14] J. Vinayagam, C. H. Balaswamy, and K. Soundararajan, “Certain Investigation on MANET Security with Routing and Blackhole Attacks Detection,” *Procedia Comput. Sci.*, vol. 165, no. 2019, pp. 196–208, 2019, doi: 10.1016/j.procs.2020.01.091.

[15] S. Karupusamy, B. Shah, A. Kumar, and P. Kanani, “An efficient intrusion detection framework for mitigating blackhole and sinkhole attacks in healthcare wireless sensor networks ☆,” *Comput. Electr. Eng.*, vol. 111, no. PB, p. 108964, 2023, doi: 10.1016/j.compeleceng.2023.108964.