EVALUASI DAMPAK SERANGAN JAMMING TERHADAP PACKET LOSS PADA PERANGKAT IOT SISTEM PERINGATAN DINI KEBOCORAN GAS LPG BERBASIS ESP32 SERTA MITIGASI MELALUI FAILOVER LORA

ABANG HUSNAL ISMAIL
H1051221086

SKRIPSI

JURUSAN REKAYASA SISTEM KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS TANJUNGPURA
PONTIANAK
2026

EVALUASI DAMPAK SERANGAN JAMMING TERHADAP PACKET LOSS PADA PERANGKAT IOT SISTEM PERINGATAN DINI KEBOCORAN GAS LPG BERBASIS ESP32 SERTA MITIGASI MELALUI FAILOVER LORA

ABANG HUSNAL ISMAIL
H1051221086

Skripsi
Sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer pada
Program Studi Rekayasa Sistem Komputer

JURUSAN REKAYASA SISTEM KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS TANJUNGPURA
PONTIANAK
2026

LEMBAR PENGESAHAN

Judul Tugas Akhir	: Evaluasi Dampak Serangan Jamming Terhadap *Packet Loss* Pada Perangkat IoT Sistem Peringatan Dini Kebocoran Gas LPG berbasis ESP32 Serta Mitigasi Melalui Failover LoRa
Nama Mahasiswa	: Abang Husnal Ismail
NIM	: H1051221086
Jurusan/Program Studi	: Rekayasa Sistem Komputer
Tanggal Lulus	: 21 Juli 2026
SK Pembimbing	: No.1019/DST/UN22.8/DT.00.09/2026/10 Maret 2026
SK Penguji	: No.4256/DST/UN22.8/DT.00.09/2026/15 Juli 2026

Dosen Pembimbing

Pembimbing I	Pembimbing II
Hirzen Hasfani, S.Kom., M.Cs.	Kasliono, S.Mat., M.Cs.
NIP. 199305032022031003	NIP. 199306202022031005

Dosen Penguji

Ketua Penguji	Anggota Penguji
Ikhwan Ruslianto, S.Kom., M.Cs	Uray Ristian, S.Kom., M.Kom
NIP. 198607012014041001	NIP. 199012012019031017

Pemimpin Sidang (merangkap anggota penguji)	Sekretaris Sidang (merangkap anggota penguji)
Hirzen Hasfani, S.Kom., M.Cs.	Kasliono, S.Mat., M.Cs.
NIP. 199305032022031003	NIP. 199306202022031005

Mengesahkan
Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Tanjungpura

Prof. Dr. Gusrizal, S.Si., M.Si.
NIP. 197108022000031001

PERNYATAAN INTEGRITAS AKADEMIK

Nama	: Abang Husnal Ismail
NIM	: H1051221086
Program Studi	: Rekayasa Sistem Komputer
Fakultas	: Matematika dan Ilmu Pengetahuan Alam

dengan ini menyatakan bahwa dokumen ilmiah Tugas Akhir yang disajikan ini tidak mengandung unsur pelanggaran integritas akademik sesuai Peraturan Menteri Pendidikan, Kebudayaan, Riset, Dan Teknologi Republik Indonesia Nomor 39 Tahun 2021. Apabila di kemudian hari dokumen ilmiah Tugas Akhir ini mengandung unsur pelanggaran integritas akademik sesuai ketentuan perundangan tersebut, maka saya bersedia menerima sanksi akademik dan/atau sanksi hukum yang berlaku.

Demikian pernyataan dapat dipergunakan sebagaimana mestinya.

Pontianak, 17 Agustus 2026



Abang Husnal Ismail
NIM. H1051221086

Evaluasi Dampak Serangan *Jamming* Terhadap *Packet Loss* pada Perangkat IoT Sistem Peringatan Dini Kebocoran Gas LPG berbasis ESP32 Serta Mitigasi Melalui *Failover* LoRa

ABSTRAK

Gas LPG yang mudah menguap berpotensi menyebabkan kebakaran atau ledakan apabila terjadi kebocoran yang tidak terdeteksi. Sistem peringatan dini berbasis ESP32 dapat digunakan sebagai solusi, namun komunikasi WiFi pada perangkat IoT rentan terhadap serangan *jamming* yang meningkatkan packet loss dan menyebabkan kegagalan pengiriman notifikasi. Penelitian ini bertujuan mengevaluasi pengaruh variasi jarak serangan *jamming* terhadap nilai packet loss serta mengevaluasi pengaruh penerapan metode *failover* menggunakan LoRa dalam meningkatkan *Message Delivery Ratio* (MDR). Penelitian ini menggunakan metode eksperimental dengan memvariasikan jarak ESP32, router, dan *jammer* masing-masing sejauh 1, 3 dan 5 meter. Data yang dikumpulkan berupa nilai packet loss, MDR, dan waktu proses *failover*, kemudian dianalisis secara deskriptif. Hasil penelitian menunjukkan bahwa nilai packet loss dipengaruhi oleh kombinasi jarak ESP32, router, dan *jammer*. Semakin jauh ESP32 dari router, komunikasi semakin rentan mengalami kegagalan akibat *jamming*. Penerapan *failover* dengan mengalihkan jalur komunikasi WiFi (2,4 GHz) ke LoRa (433 MHz) terbukti berhasil meningkatkan nilai MDR dari 0% menjadi 100% dengan mengirim ulang pesan yang gagal pada pengujian yang dilakukan, meskipun menambah waktu pengiriman. Dengan demikian, metode *failover* mampu meningkatkan keandalan sistem peringatan dini dengan menjaga keberlangsungan pengiriman notifikasi ketika komunikasi WiFi terganggu akibat serangan *jamming*.

Kata kunci: Kebocoran gas LPG, ESP32, *Jamming*, *Packet Loss*, *Failover*, LoRa.

Evaluasi Dampak Serangan *Jamming* Terhadap *Packet Loss* pada Perangkat IoT Sistem Peringatan Dini Kebocoran Gas LPG berbasis ESP32 Serta Mitigasi Melalui *Failover* LoRa

ABSTRACT

Liquefied Petroleum Gas (LPG) poses a significant risk of fire or explosion if leaks remain undetected. While ESP32-based early warning systems offer a viable solution, the reliance of Internet of Things (IoT) devices on WiFi communication makes them highly vulnerable to jamming attacks, which increase packet loss and lead to notification delivery failures. This study aims to evaluate the impact of varying jamming attack distances on packet loss and to assess the effectiveness of implementing a LoRa-based failover method in improving the Message Delivery Ratio (MDR). An experimental method was employed by varying the distances between the ESP32, router, and jammer at 1, 3 and 5 meters. The collected data—comprising packet loss, MDR, and failover processing time—were analyzed descriptively. The results indicate that packet loss is significantly influenced by the spatial configuration of the ESP32, router, and jammer; the further the ESP32 is from the router, the more susceptible the communication is to failure due to jamming. The implementation of the failover mechanism, which switches the communication pathway from WiFi (2.4 GHz) to LoRa (433 MHz), successfully increased the MDR from 0% to 100% by resending failed messages during the tests, albeit with an increase in transmission time. Thus, the failover method effectively enhances the reliability of the early warning system by ensuring continuous notification delivery when the primary WiFi communication is disrupted by jamming attacks.

Keywords: *LPG Leak Detection, ESP32, Jamming, Packet Loss, Failover, LoRa.*

PRAKATA

Alhamdulillah, segala puji syukur penulis ucapkan kehadirat Allah Subhanahu Wa Ta'ala serta nabi besar Muhammad Shallallahu'alaihi Wa Sallam karena atas rahmat dan hidayah-nya, sehingga penulis dapat menyelesaikan tugas akhir yang berjudul **"Evaluasi Dampak Serangan *Jamming* Terhadap *Packet Loss* pada Perangkat IoT Sistem Peringatan Dini Kebocoran Gas LPG berbasis ESP32 Serta Mitigasi Melalui *Failover* LoRa"**.

Tujuan dari penyusunan skripsi ini guna memenuhi salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom) pada Program Studi Rekayasa Sistem Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura.

Penulis menyadari bahwa dalam penulisan laporan ini banyak mengalami kendala. Namun, dalam penyelesaian penulisan ini tidak terlepas dari bimbingan, pengarahan, saran, dan bantuan moril maupun material dari berbagai pihak. Untuk itu penulis mengucapkan terima kasih yang tak terhingga kepada:

1. Bapak Prof. Dr. Gusrizal, S.Si., M.Si., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura.
2. Ibu Rahmi Hidayati, S.Kom., M.Cs., selaku Ketua Jurusan/Program Studi Rekayasa Sistem Komputer.
3. Bapak Hirzen Hasfani, S.Kom., M.Cs., selaku Dosen Pembimbing Akademik sekaligus Pembimbing Utama yang telah memberikan petunjuk, bimbingan, dan pengarahan dalam penyusunan skripsi ini.
4. Bapak Kasliono, S.Mat., M.Cs., selaku Dosen Pembimbing Pendamping yang telah memberikan petunjuk, bimbingan, dan pengarahan dalam penyusunan skripsi ini.
5. Bapak Ikhwan Ruslianto, S.Kom., M.Cs., selaku Dosen Penguji Pertama yang telah memberikan saran dan masukan dalam penulisan skripsi ini.
6. Bapak Uray Ristian, S.Kom., M.Kom., selaku Dosen Penguji Kedua yang telah memberikan saran dan masukan dalam penulisan skripsi ini.

7. Seluruh dosen dan staf Jurusan Rekayasa Sistem Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Tanjungpura, yang telah memberikan ilmu, bantuan, serta dukungan selama masa perkuliahan.
8. Seluruh staf dan anggota bagian akademik Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Tanjungpura, yang telah memberikan pelayanan, bantuan administrasi, serta kemudahan dalam mengurus berbagai keperluan akademik selama masa perkuliahan.
9. Kepada orang tua penulis yang selalu memberikan dukungan, doa, motivasi, dan kasih sayang tanpa henti sepanjang perjalanan penulisan tugas akhir ini
10. Kepada teman-teman terbaik Mabar The Ghost (TGO Company) yaitu Ahnaf Fikriyansyah, Arya Ridho Yudhistira, Fajar Muttaqien Aska dan Alvin Nataniel, yang tidak pernah lelah menemani dan memberi dukungan serta membantu dalam pengambilan data maupun memberi masukan terkait penyusunan skripsi ini.
11. Teman-teman seperjuangan mahasiswa Jurusan/Program Studi Rekayasa Sistem Komputer angkatan 2022 Cytigon yang telah berjuang bersama selama masa perkuliahan yang tidak bisa disebut satu per satu.
12. Semua pihak yang tidak dapat disebutkan satu per satu yang turut membantu dalam penyusunan skripsi ini baik secara langsung maupun tidak langsung.

Pontianak, 17 Agustus 2026

Abang Husnal Ismail
NIM. H1051221086

DAFTAR ISI

LEMBAR PENGESAHAN ii
PERNYATAAN INTEGRITAS AKADEMIK iii
ABSTRAK iv
ABSTRACT v
PRAKATA vi
DAFTAR ISI viii
DAFTAR GAMBAR xi
DAFTAR TABEL xii
DAFTAR KODE PROGRAM xiii
BAB 1 PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Rumusan Masalah 4
1.3. Batasan Masalah 4
1.4. Tujuan Penelitian 5
1.5. Manfaat Penelitian 5
1.6. Sistematika Penulisan 6
BAB 2 LANDASAN TEORI 8
2.1. Perbandingan Dengan Penelitian Terdahulu 8
2.2. Mikrokontroler ESP32 8
2.3. LoRa 9
2.4. NRF24L01 10
2.5. M5Stack Cardputer 10
2.6. Sensor MQ-6 11
2.7. Gas LPG 12
2.8. Telegram 12
2.9. Arduino IDE 12
2.10. Bruce Firmware 13
2.11. *Jamming* 13
2.11.1. Pengertian *Jamming* 13

2.11.2. Jenis-Jenis *Jamming* 13
2.12. *Packet Loss* 15
2.13. *Message Delivery Ratio* 16
2.14. Perangkat IoT 16
2.15. Metode *Failover* 16
2.16. WiFi 16
2.17. *Beacon frame* 17
2.18. *Flowchart* 17
BAB 3 METODE PENELITIAN 18
3.1. Studi Literatur 19
3.2. Analisis Kebutuhan 19
3.2.1. Kebutuhan Perangkat Keras 19
3.2.2. Kebutuhan Perangkat Lunak 19
3.3. Perancangan Sistem 20
3.3.1. Perancangan Perangkat Keras 20
3.3.2. Perancangan Perangkat Lunak 20
3.4. Implementasi Sistem 20
3.5. Pengujian 20
3.6. Analisis Hasil 21
3.7. Kesimpulan dan Saran 21
BAB 4 PERANCANGAN 22
4.1. Deskripsi Sistem 22
4.2. Perancangan Arsitektur Sistem 23
4.3. Perancangan Perangkat Keras 24
4.3.1. Perancangan Sistem Peringatan Dini Kebocoran Gas LPG 24
4.3.2. Perancangan Perangkat LoRa *Receiver* 26
4.3.3. Perancangan *Tools Jamming* 28
4.4. Perancangan perangkat Lunak 30
4.4.1. Perancangan Pengukuran *Packet Loss* 32
4.4.2. Perancangan Pengujian *Failover* 33
4.5. Perancangan Antarmuka Telegram Bot 34
4.6. Perancangan Pengujian Keseluruhan Sistem 34

4.7. Perancangan Pengujian Variasi Jarak Serangan *Jamming* 35
4.8. Perancangan Pengujian Metode *Failover* 36
BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN.....38
5.1. Implementasi Perangkat Keras.....38
5.1.1. Implementasi Sistem Peringatan Dini Kebocoran Gas LPG.....38
5.1.2. Implementasi Perangkat LoRa *Receiver* 39
5.1.3. Implementasi *Tools Jamming* 40
5.2. Implementasi Perangkat Lunak.....41
5.2.1. Implementasi Pengukuran *Packet Loss*.....42
5.2.2. Implementasi Pengujian *Failover* 42
5.3. Implementasi Antarmuka 44
5.4. Pengujian Keseluruhan Sistem.....45
5.5. Pengujian Variasi Jarak Serangan *Jamming* 46
5.6. Pengujian Metode *Failover*.....50
5.7. Pembahasan.....53
BAB 6 PENUTUP 58
6.1. Kesimpulan.....58
6.2. Saran.....59
DAFTAR PUSTAKA 60
LAMPIRAN.....65

DAFTAR GAMBAR

Gambar 2.1 ESP32 9
Gambar 2.2 LoRa 9
Gambar 2.3 NRF24L01 10
Gambar 2.4 M5Stack Cardputer 11
Gambar 2.5 Sensor MQ-6 11
Gambar 2.6 Gas LPG 12
Gambar 2.7 Arduino IDE 13
Gambar 3.1 Flowchart Alur Penelitian 18
Gambar 4.1 Arsitektur Sistem 23
Gambar 4.2 Rancangan Sistem Peringatan Dini Kebocoran Gas LPG 25
Gambar 4.3 Rancangan Perangkat LoRa Receiver 27
Gambar 4.4 Perancangan tools *Jamming* 29
Gambar 4.5 Flowchart Perangkat Lunak 31
Gambar 4.6 Flowchart Pengukuran Packet Loss 32
Gambar 4.7 Flowchart Pengujian Failover 33
Gambar 4.8 Ilustrasi Antarmuka Menggunakan Telegram Bot 34
Gambar 5.1 Implementasi Sistem Peringatan Dini Kebocoran Gas LPG 39
Gambar 5.2 Implementasi LoRa Receiver 40
Gambar 5.3 Implementasi tools Jamming 41
Gambar 5.4 Tampilan Antarmuka Telegram 44
Gambar 5.5 Skenario Pengujian Variasi Jarak Serangan Jamming 46
Gambar 5.6 Pesan Pada Telegram Yang Diteruskan Oleh LoRa Receiver 51

DAFTAR TABEL

Tabel 2.1 Perbandingan dengan Penelitian Terdahulu.....8
Tabel 2.2 Standar Packet Loss 15
Tabel 2.3 Simbol-simbol flowchart.....17
Tabel 4.1 Penggunaan Pin ESP32 pada Sensor MQ-6 dan LoRa Transmitter 25
Tabel 4.2 penggunaan pin ESP32 pada LoRa Receiver.....27
Tabel 4.3 Penggunaan Pin M5Stack Cardputer Dengan NRF24L01.....29
Tabel 4.4 Skenario Pengujian Keseluruhan Sistem 35
Tabel 4.5 Pengujian Variasi Jarak Serangan *Jamming* 36
Tabel 4.6 Skenario Pengujian MDR 37
Tabel 5.1 Ringkasan Hasil Pengujian Keseluruhan Sistem 45
Tabel 5.2 Bukti Log Pengujian Variasi Jarak Serangan *Jamming*.....47
Tabel 5.3 Ringkasan Hasil Pengujian Variasi Jarak Serangan *Jamming*.....49
Tabel 5.4 Bukti Log Isi Pesan Pada Pengujian Metode Failover.....50
Tabel 5.5 Hasil Pengujian Metode Failover.....53

DAFTAR KODE PROGRAM

Kode Program 5.1 Pengukuran Packet Loss 42
Kode Program 5.2 Pengujian Failover 43

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Gas (LPG) merupakan campuran hidrokarbon berupa propana dan butana yang mudah menguap pada suhu di atas 24°C dan sangat berbahaya apabila terjadi kebocoran di ruang tertutup, terutama jika suhu mencapai lebih dari 30°C. Kebocoran gas yang tidak terdeteksi dapat memicu ledakan atau kebakaran yang berakibat fatal bagi penghuni rumah maupun lingkungan sekitar. Penyebab kebocoran gas umumnya berasal dari kerusakan selang, regulator yang tidak terpasang dengan baik, karet pengaman yang aus, hingga cacat produksi tabung gas (Fauzi & Sukarno, 2025). Pemanfaatan Internet of Things (IoT) menjadi salah satu solusi dalam mengembangkan sistem peringatan dini. Konsep saling terhubung secara nirkabel dan luas yang dihadirkan oleh IoT memungkinkan perangkat sensor untuk mendeteksi kondisi lingkungan dan mengirimkan informasi secara otomatis kepada pengguna kapan saja dan di mana saja melalui berbagai jaringan dan layanan yang tersedia, sehingga memfasilitasi pertukaran data yang *real-time* (Wibowo et al., 2023). Salah satu mikrokontroler yang sering digunakan dalam perangkat IoT tersebut adalah ESP32. perangkat mikrokontroler seperti ESP32 menjadi pilihan yang populer karena memiliki System on Chip (SoC) yang mendukung koneksi WiFi tanpa memerlukan perangkat tambahan, sehingga ideal untuk sistem monitoring jarak jauh maupun sistem keamanan rumah. Namun, di balik keunggulannya, komunikasi nirkabel pada ESP32 yang umumnya mengandalkan jaringan WiFi memiliki kerentanan terhadap ancaman keamanan, khususnya serangan *jamming*. Serangan *jamming* adalah serangan yang menargetkan lapisan fisik yang dilakukan dengan memancarkan radio pengganggu pada frekuensi yang sama sehingga perangkat yang saling terhubung tidak dapat berkomunikasi (Sabbar Jasim et al., 2023). Dampak dari serangan ini cukup serius karena sistem yang seharusnya bekerja otomatis menjadi tidak dapat diandalkan sepenuhnya misalnya, sensor gagal mengirim data, notifikasi peringatan tidak sampai, atau perintah aktuator tidak terlaksana (França et al., 2021). Kegagalan

pengiriman data akibat gangguan sinyal ini secara teknis berdampak langsung pada peningkatan rasio *packet loss*. Tingginya *packet loss* sangat krusial dalam sistem peringatan dini, karena menandakan hilangnya paket informasi yang seharusnya diterima pengguna. Apabila gangguan tersebut terjadi secara terus-menerus, maka *availability* dan efektivitas pemanfaatan IoT akan berkurang (Muhammad Rizal et al., 2023). Oleh karena itu, diperlukan evaluasi secara menyeluruh untuk mengetahui dampak dari serangan *jamming* terhadap *packet loss*, sekaligus diperlukan solusi atau mekanisme mitigasi yang mampu meningkatkan keandalan komunikasi IoT agar sistem tetap berfungsi meskipun mengalami gangguan *jamming*.

Salah satu upaya mitigasi untuk mengatasi gangguan komunikasi nirkabel akibat serangan *jamming* tersebut adalah dengan mengimplementasikan *failover* yang mampu menjaga keberlangsungan komunikasi secara otomatis ketika koneksi utama pada perangkat IoT yakni modul ESP32 terganggu oleh serangan *jamming*. *failover* ini merupakan mekanisme yang memungkinkan sistem tetap beroperasi dengan cara mengalihkan fungsi layanan atau komunikasi ke jalur cadangan ketika jalur utama mengalami kegagalan (Putra Raharjo & Setiawan, 2024). Dalam implementasinya, teknologi LoRa (*Long Range*) digunakan sebagai kanal alternatif cadangan. LoRa sendiri merupakan teknologi nirkabel hemat daya yang dirancang untuk komunikasi jarak jauh dengan memanfaatkan *Chirp Spread Spectrum* yang membuat LoRa juga lebih tahan terhadap *noise* (Kusyanti et al., 2023).

Adapun penelitian sebelumnya yang terkait, dengan judul "Analisis Serangan *Jammer* Pada Jaringan Wireless" (Djamin et al., 2025). Penelitian tersebut mengevaluasi efektivitas serangan *jamming* dan dampaknya terhadap performa serta keamanan jaringan nirkabel. Pengujian dilakukan melalui *penetration testing*, yang dimana serangan *jamming* ini memanfaatkan *tools* Fluxion yang menerapkan teknik *deauthentication* pada protokol WiFi untuk mengganggu komunikasi antara perangkat dan *Access Point*. Hasil penelitian menunjukkan bahwa serangan *jamming* dapat secara signifikan menurunkan kualitas layanan dan menyebabkan gangguan serius terhadap kestabilan jaringan. Selain itu, Penelitian ini menunjukkan bahwa strategi keamanan yang tepat dapat mengurangi dampak serangan *jamming* dan menjaga kestabilan jaringan.

Penelitian kedua dengan judul "*Anti Jamming Low Latency Channel Hopping Protocol for Cognitive Radio Networks*" (Hsieh et al., 2023). Penelitian ini berfokus pada pengembangan dan evaluasi protokol channel hopping anti *jamming* pada *Cognitive Radio Network* (CRN) untuk meningkatkan peluang komunikasi antar pengguna serta meminimalkan waktu pertemuan kanal (Time to Rendezvous). Protokol yang diusulkan, yaitu *Anti jamming Low Latency* (ALL), dirancang dengan menyesuaikan struktur matriks channel hopping antara pengirim dan penerima guna meningkatkan probabilitas rendezvous sekaligus menjaga ketahanan terhadap serangan *jamming*. Hasil simulasi menunjukkan bahwa protokol ALL mampu meningkatkan network throughput dan mengurangi TTR secara signifikan dibandingkan metode sebelumnya, dengan peningkatan performa rata-rata masing-masing sebesar 25% dan 20%.

Penelitian selanjutnya dengan judul "Perancangan Dan Implementasi Server Backup Menggunakan Metode *Failover*" (Karneli et al., 2024). Penelitian ini merancang sistem server backup menggunakan sistem operasi Linux Ubuntu Server 18.04 dan database MySQL dengan pendekatan metode *failover* dan teknik replikasi master to master. Server A dan Server B saling mereplikasi data melalui jaringan lokal untuk menjaga ketersediaan dan keamanan data secara *real-time*, khususnya dalam konteks penyimpanan data internal dan eksternal yang besar seperti pada Dinas Komunikasi dan Informatika serta lingkungan sekolah (SMK S1 Pembangunan Kota Bengkulu). Hasil penelitian menunjukkan bahwa sistem berhasil melakukan replikasi dan backup secara otomatis dengan waktu sinkronisasi data antara 2-10 detik. Selain itu, sistem mampu melakukan perpindahan layanan dari server utama ke server cadangan secara otomatis saat terjadi gangguan tanpa memerlukan konfigurasi ulang, sehingga metode *failover* dapat menjaga kontinuitas layanan dan integritas data.

Berdasarkan latar belakang penelitian-penelitian terkait, maka dilakukan penelitian berjudul "Evaluasi Dampak Serangan *Jamming* Terhadap *Packet Loss* pada Perangkat IoT Sistem Peringatan Dini Kebocoran Gas LPG berbasis ESP32 Serta Mitigasi Melalui *Failover* LoRa".

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka didapatlah rumusan permasalahan sebagai berikut:

1. Bagaimana pengaruh variasi jarak serangan *jamming* terhadap nilai *packet loss* pada komunikasi perangkat IoT berbasis ESP32?
2. Bagaimana pengaruh penerapan metode *failover* dalam meningkatkan nilai *Message Delivery Ratio* (MDR) pada pengiriman pesan oleh perangkat IoT saat terjadi serangan *jamming*?

1.3. Batasan Masalah

Dalam penelitian ini diterapkan ruang lingkup batasan agar tetap fokus pada pokok masalah dan mempermudah pembahasan supaya tujuan penelitian tercapai, maka diberikan batasan masalah sebagai berikut:

1. Studi kasus pada penelitian ini adalah sistem pendeteksi kebocoran dini gas LPG dengan sensor MQ-6, ESP32 dan tidak membahas akurasi sensor secara mendalam.
2. Metrik yang diukur pada penelitian ini adalah *packet loss*, variasi *distance* (jarak) dan *Message Delivery Ratio.*
3. Alat *jamming* yang digunakan dalam penelitian ini menggunakan M5Stack Cardputer yang terinstalasi firmware bruce serta dilengkapi dengan dua NRF24L01.
4. Serangan *jamming* difokuskan menghasilkan gangguan pada pita frekuensi 2,4 GHz secara konstan yang menargetkan ESP32 yang terhubung ke jaringan WiFi.
5. Solusi yang diberikan merupakan metode *failover* yang beralih dari komunikasi utama dari WiFi dengan frekuensi 2,4 GHz dipindahkan ke komunikasi cadangan yakni LoRa dengan frekuensi 433 MHz.
6. Sistem komunikasi terdiri dari dua node: LoRa *transmitter* yang mengirimkan notifikasi yang dipasangkan pada perangkat IoT saat terjadi serangan *jamming* yang dipasangkan ke sistem peringatan dini kebocoran gas LPG, dan LoRa *receiver* (penerima) yang akan meneruskan pesan tersebut ketika terjadi kegagalan dalam pengiriman notifikasi saat terjadi serangan *jamming*.

7. Sistem pemantauan atau notifikasi dibangun menggunakan platform Telegram, yang berfungsi untuk menyampaikan peringatan kepada pengguna secara *real-time*.
8. Transmisi data dilakukan melalui jaringan WiFi lokal (provider indihome) dengan bandwidth 73 Mbps.
9. Jumlah data pengujian dibatasi berdasarkan jenis pengujian, yaitu 30 percobaan untuk setiap skenario pengujian keseluruhan sistem, 100 paket data pada setiap kombinasi jarak untuk pengujian packet loss, serta 10 pesan notifikasi pada pengujian metode *failover*. Variasi jarak dibatasi pada 1, 3 dan 5 meter dengan pengujian dilakukan di ruangan tertutup tanpa halangan.
10. Penelitian ini berfokus untuk mengevaluasi dampak serangan *jamming* terhadap packet loss berdasarkan variasi jarak serangan, dan mengevaluasi kemampuan metode *failover* dalam meningkatkan kembali nilai MDR ketika terjadi serangan *jamming*. Penelitian ini tidak membahas aspek keamanan data, seperti kerahasiaan, autentikasi, maupun integritas data, *jamming* terhadap LoRa, maupun gangguan WiFi yang umumnya sering terjadi.

1.4. Tujuan Penelitian

Berdasarkan rumusan permasalahan, penelitian ini memiliki tujuan sebagai berikut:

1. Mengetahui pengaruh variasi jarak serangan *jamming* terhadap nilai *packet loss* pada komunikasi perangkat IoT.
2. Mengetahui pengaruh penerapan metode *failover* dalam meningkatkan nilai *Message Delivery Ratio* (MDR) pada pengiriman pesan oleh perangkat IoT saat terjadi serangan *jamming*.

1.5. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan informasi mengenai pengaruh variasi jarak serangan *jamming* terhadap nilai *packet loss* pada komunikasi perangkat IoT berbasis ESP32. Selain itu, penelitian ini juga diharapkan dapat menjadi referensi mengenai bagaimana pengaruh penerapan metode *failover* dengan memanfaatkan jalur komunikasi alternatif melalui LoRa dalam

meningkatkan nilai *Message Delivery Ratio* pada pengiriman pesan perangkat IoT saat terjadi serangan *jamming*.

1.6. Sistematika Penulisan

Skripsi ini disusun ke dalam 6 bab agar pembahasan penelitian dapat disajikan secara sistematis dan terstruktur. Setiap bab memuat pembahasan yang saling berkaitan, mulai dari latar belakang penelitian, landasan teori, metode penelitian, hasil dan pembahasan, hingga kesimpulan dan saran. Adapun sistematika penulisan skripsi ini terdiri dari:

BAB 1 PENDAHULUAN

Bab pendahuluan berisi latar belakang mengenai kerentanan pada perangkat IoT akibat serangan *jamming* dan latar belakang dilakukannya penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Bab landasan teori berisi bahasan mengenai dasar teori pendukung yang digunakan dalam tugas akhir. Landasan teori meliputi perbandingan dengan penelitian terdahulu, mikrokontroler ESP32, LoRa, NRF24L01, M5Stack Cardputer, sensor MQ-6, Gas LPG, Telegram, Arduino IDE, Bruce Firmware, konsep serangan *jamming*, *packet loss*, *Message Delivery Ratio*, perangkat IoT, metode *failover*, WiFi status, beacon frame, serta *flowchart*.

BAB 3 METODE PENELITIAN

Bab metode penelitian menjelaskan prosedur penelitian yang dilakukan untuk mengumpulkan dan menganalisis data serta menjawab pertanyaan atau hipotesis yang telah ditetapkan dalam penelitian. Adapun isi dimulai dari metode penelitian yaitu diagram alir, studi literatur, analisis kebutuhan, perancangan sistem, pengujian sistem, data hasil pengujian, kesimpulan dan saran.

BAB 4 PERANCANGAN

Bab perancangan berisi secara rinci tentang perancangan dan tahapan dalam melakukan penelitian. Pada bab ini secara umum meliputi perancangan pada perangkat keras, perangkat lunak, perancangan antarmuka dan perancangan pengujian sistem.

BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN

Bab implementasi, pengujian dan pembahasan membahas mengenai analisis dan implementasi sistem yang telah dirancang pada tahap sebelumnya. Tahapan ini meliputi implementasi perangkat keras, implementasi perangkat lunak, pengujian, dan pembahasan.

BAB 6 PENUTUP

Pada bab penutup merupakan bab yang membahas terkait kesimpulan dari bahasan masalah pada bab-bab sebelumnya serta saran terhadap masalah yang belum terselesaikan untuk dapat diperbaiki dan dikembangkan pada penelitian berikutnya.