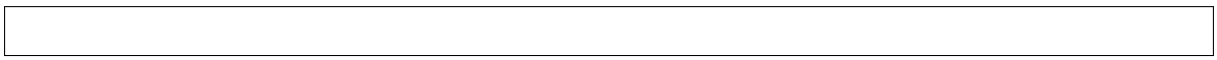
Diploma Project

Detecting Jamming Attacks in Lorawan IoT using Fuzzy Logic

Elena Alexandrou

University of Cyprus
Department of Computer Science

Department of Computer Science



UNIVERSITY OF CYPRUS

Faculty of Pure and Applied Sciences

Department of Computer Science

Detecting Jamming Attacks in Lorawan IoT using Fuzzy Logic

Elena Alexandrou

Advisor:

Dr Vasos Vasiliou

The Thesis was submitted in partial fulfillment of the requirements for obtaining the Computer Science degree of the Department of Computer Science of the University of Cyprus

May 2025

Acknowledgements

I would like to sincerely thank my professor, **Dr. Vasos Vasileiou**, for his invaluable guidance, continuous support, and constructive feedback throughout the course of this project. His expertise and encouragement were instrumental in shaping the direction and quality of this work.

I am also deeply grateful to **Dr. Michalis Savva** for his insightful suggestions and assistance during the development and evaluation stages. His support was especially appreciated during these times and especially in the implementation process.

ABSTRACT

Wireless sensor networks (WSNs) and Internet of Things (IoT) systems are increasingly deployed in critical environments, yet they remain vulnerable to jamming attacks that can severely disrupt communication by interfering with radio transmissions. This threat is particularly serious in resource-constrained settings such as LoRaWAN networks, where complex security mechanisms may not be feasible. As a result, there is a growing need for lightweight, interpretable detection approaches that can operate under uncertain and dynamic conditions.

This study investigates the suitability of fuzzy logic-based systems for detecting jamming in such environments. Specifically, it evaluates whether fuzzy inference systems (FIS) can effectively use physical- and link-layer metrics to compute a continuous jamming likelihood score.

Multiple fuzzy rule and membership function sets were developed and tested across various input combinations, with detection performance assessed using accuracy, precision, recall, and F1 score. Results indicate that fuzzy logic offers a promising detection framework, especially when using PLR, which improved detection outcomes. However, effectiveness also depends on data quality, as feature overlap between normal and jammed signals in the dataset limited performance in certain cases.

Keywords: Fuzzy Logic, Jamming Detection, IoT Security, LoRaWAN, Intrusion Detection System, Wireless Sensor Networks

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Important abbreviations that have been used in the text and need explanation are briefly presented.

WSN	Wireless Sensor Networks
IoT	Internet of Things
LoRaWAN	Long Range Wide Area Network
CSS	Chirp Spread Spectrum
ADR	Adaptive Data Rate
RSSI	Received Signal Strength Indicator
SNR	Signal-to-Noise Ratio
SDR	Software-defined Radio
PLR	Packet Loss Rate
JI	Jamming Index
FIS	Fuzzy Inference System

1 Chapter 1

Introduction

The rapid growth of IoT and WSNs has enabled smarter systems but also introduced security risks, particularly jamming attacks that disrupt wireless communications. LoRaWAN, a widely used low-power, long-range protocol, is especially vulnerable due to its simple ALOHA-based access and slow transmissions. This research develops a lightweight, fuzzy logic-based method to detect jamming in resource-constrained LoRaWAN networks.

1.1 Motivation

The advent of the Internet of Things (IoT) and Wireless Sensor Networks (WSNs) has sparked significant technological advancements, fundamentally changing the way we interact with our environment and manage systems. These technologies enable the collection, sharing, and analysis of data across various industries, leading to smarter, more efficient solutions. Applications in fields such as smart cities, industrial automation, healthcare and environmental monitoring are powered by IoT and WSNs, which provide previously unachievable real-time insights and automation [6] [7] [8]. By improving operational effectiveness, resource allocation, and decision-making, these skills have the potential to revolutionize daily life.

Although IoT and WSN have many advantages, there are a number of security issues related to their wide use. These systems are vulnerable to a variety of undesirable actions, as they are frequently implemented in open, unprotected scenarios, which can seriously compromise their reliability, functionality, and credibility. Jamming attacks are among the most urgent security risks. The communication links that are essential for both IoT and WSN systems are the specific target of these attacks. Jamming attacks can seriously impair system performance or, in certain situations, make the entire system unusable by interfering with wireless signals or introducing interference.

This research is driven by the need to understand and address the impact of jamming attacks on the performance and security of IoT and WSN systems. Although a wide body of literature addresses general IoT security, relatively fewer studies offer comprehensive experimental evaluations of physical-layer jamming detection in constrained environments, especially within low-power long-range protocols like LoRaWAN and NB-IoT. LoRaWAN's long-range, low-power design makes it ideal for IoT applications, but its simplicity also creates security weaknesses. Its reliance on basic protocols like ALOHA (which has no collision protection), slow transmis-

sion speeds (making signals easy to disrupt), and reliance on a single gateway (a single point of failure) make it an attractive target for jamming, replay, and spoofing attacks[9] [10].

A key motivation for selecting LoRaWAN as the experimental platform is its role as a practical bridge between IoT and WSN technologies. It combines the long-range, low-power capabilities typical of WSNs with the scalability and flexibility of modern IoT systems. LoRaWAN has seen widespread adoption in smart agriculture, industrial IoT, smart grids, and environmental monitoring due to its ability to maintain low energy consumption across enormous distances [11]. It is a perfect choice for investigating the real-world impacts of jamming and creating innovative detection techniques due to its simple access to the channel and weak defenses of the physical layer [9].

By investigating jamming through a combination of signal analysis, fuzzy logic techniques, and real-world experimentation on constrained LoRa-based nodes, this thesis aims to bridge the gap between theoretical security models and practical applications. The use of fuzzy logic enables the development of lightweight, interpretable, and adaptive decision-making systems capable of operating under uncertainty, an inherent characteristic of the behavior of wireless signals in real-world environments.

Designing and evaluating low-complexity jamming detection techniques that can be deployed on resource-constrained IoT and WSN platforms—where conventional, heavyweight intrusion detection systems are often impractical—is the central motivation of this work. This effort is driven by both academic curiosity and practical necessity. By employing fuzzy inference techniques, the proposed method provides a flexible and interpretable approach to distinguishing between normal and jammed conditions using continuous-valued physical-layer signal measurements.

In addition, this research is driven by the growing demand from both industry and academia to secure the wireless communication backbone of increasingly dense and mission-critical digital infrastructures. As the number of connected devices continues to increase, so does the potential impact of jamming attacks on network availability and data integrity. Providing experimentally validated insights, performance metrics, and adaptable detection frameworks directly contributes to the development of more resilient and secure wireless systems.

Ultimately, this thesis seeks to advance jamming detection by implementing, evaluating, and analyzing fuzzy logic–based detection strategies in realistic, constrained IoT and WSN scenarios, with a focus on LoRaWAN environments.

1.2 Problem Description

While the use of IoT and WSN devices is being adopted in different areas, their wireless mode of communication exposes them to interference-based risks. Among these, jamming attacks

are particularly disruptive, targeting the physical layer to block or degrade communication between devices. These attacks pose significant dangers in industries such as healthcare, industrial automation, and environmental monitoring as they can impair network availability, delay the delivery of vital data, and in certain situations, entirely prevent systems from operating.

Real-world incidents have demonstrated the severity of these threats. Incidents in the real world have shown how serious these threats are. Air traffic control in Sweden was severely disrupted by GPS jamming in 2015, which grounded flights and demonstrated how radio interference may seriously damage vital infrastructure [12]. Similarly, researchers showed that inexpensive jammers may turn off keyless automobile entry systems, making it possible to steal a car without physically entering it [13]. Moreover, research has demonstrated that jamming can disrupt production processes and raise safety concerns in industrial settings by interfering with sensor-controller links [14]. These examples highlight the viability and risk of jamming attacks in the real world when they target systems that rely on wireless communication.

Despite the fact that jamming is an acknowledged danger, the majority of current solutions concentrate on mitigation rather than detection, and many of them make unreasonable assumptions about the availability of computing or communication resources for limited IoT and WSN devices. Additionally, there is currently a lack of established lightweight, real-time detection techniques that are practical and deployable in low-power real-world settings.

Specifically, protocols like LoRaWAN, which are popular because of their long-range and energy-efficient capabilities, are intrinsically susceptible to jamming due to their weak physical-layer protections and basic ALOHA-based MAC layer [10]. Due to these drawbacks, LoRaWAN is a perfect but underutilized platform for analyzing detection tactics and examining actual jamming behavior.

Another key challenge is the statistical imbalance in real-world datasets, where jamming events are rare compared to normal network traffic. This class imbalance makes traditional classification techniques and evaluation metrics inadequate or misleading.

Given these limitations, there is a clear need for a practical, lightweight, and experimentally validated jamming detection approach that:

- Operates effectively in constrained environments like those of LoRaWAN-based IoT and WSN systems.
- Utilizes physical-layer signal features available on commodity devices.
- Handles data imbalance and uncertainty in wireless environments.

This thesis addresses this problem by developing and evaluating a fuzzy logic–based detection framework that meets the above criteria. It aims to contribute both theoretical insights and practical tools for improving the resilience of low-power wireless networks against jamming

threats.

1.3 Thesis Structure

This thesis is organized into five chapters, each addressing a specific aspect of the research problem, from conceptual background to experimental evaluation and final conclusions:

- **Chapter 1 – Introduction:** Introduces the research problem, outlines the importance of jamming detection in IoT and WSN environments, and discusses the motivation behind selecting LoRaWAN as the experimental platform. It also presents the objectives and scope of the thesis.
- **Chapter 2 – Background and Related Work:** Reviews the core concepts of wireless sensor networks, IoT architectures, LoRaWAN, jamming attacks, and physical-layer vulnerabilities. It also discusses existing detection and mitigation techniques, as well as previous work on LoRaWAN and fuzzy logic in network security.
- **Chapter 3 – Methodology and Implementation:** Describes the preprocessing and exploration of the real-world LoRaWAN dataset, including the characteristics of RSSI, SNR, and PLR. It details the design of the fuzzy inference system for each input combination, including the definition of fuzzy membership functions and output mappings. This chapter establishes the modeling framework used in the detection experiments.
- **Chapter 4 – Experimental Scenarios and Evaluation:** Evaluates the fuzzy logic–based detection framework by testing multiple rule set variations for each input combination (RSSI, SNR, PLR). It presents quantitative results using accuracy, precision, recall, and F1 score, and discusses how rule design, feature selection, and class imbalance affect detection performance.
- **Chapter 5 – Conclusions and Future Work:** Summarizes the key findings, discusses limitations, and outlines potential directions for future research in lightweight intrusion detection and physical-layer security for IoT and WSN deployments.

2 Chapter 2

Background and Related Work

This chapter outlines the essential concepts and existing research relevant to this thesis. This chapter begins by introducing Wireless Sensor Networks (WSNs), the Internet of Things (IoT), and the LoRaWAN protocol, emphasizing their roles in enabling low-power, long-range communication in modern distributed systems. It then examines jamming attacks, focusing on their operational mechanisms and the disruption they cause to wireless networks.

The chapter examines current jamming attack detection and mitigation strategies for WSN, IoT, and LoRaWAN systems, emphasizing simple approaches that can be implemented on devices with limited resources. Finally, it explores earlier studies on the use of fuzzy logic in network security contexts and talks about the weaknesses of existing methods, especially in LoRaWAN situations.

2.1 Background

2.1.1 Wireless Sensor Networks

Wireless Sensor Networks (WSNs) are decentralized systems as illustrated in Figure 2.1 of numerous spatially distributed sensor nodes that cooperatively monitor physical or environmental parameters such as temperature, humidity, sound, pressure, light, or motion [15]. These nodes are typically equipped with a sensing unit, a microcontroller for local data processing, a wireless transceiver for communication, and a power source—often a battery with limited capacity [16].

WSNs are designed to operate autonomously with minimal human intervention. To send data to a central base station (sink node), the sensor nodes can communicate directly or through multi-hop routing protocols. There, the data is compiled, examined, and possibly sent to cloud platforms or other systems for additional processing [15]. Typically, the network structure is self-organizing and ad hoc, dynamically adjusting to variations in node mobility, energy levels, and availability.

WSNs are widely used in diverse application domains including environmental monitoring (e.g., forest fire detection, pollution tracking), industrial automation (e.g., equipment fault diagnosis), precision agriculture (e.g., soil moisture sensing), smart homes and buildings, health monitoring systems, and military surveillance [16] [15]. Their deployment in often remote or inaccessible environments makes them invaluable for continuous and scalable data acquisition in real-time.

The resource-constrained nature of WSN nodes presents a number of challenges, such as short battery life, little memory, and restricted processing power [17]. The design of data aggregation techniques, energy-efficient routing, and communication protocols are all greatly impacted by these constraints. Furthermore, WSNs are extremely susceptible to a number of safety threats due to their dependence on wireless communication and lack of centralized infrastructure [17], including eavesdropping, data tampering, node capture, spoofing, and physical-layer attacks like jamming.

Jamming attacks are especially problematic for WSNs because they directly target the wireless communication channel, disrupting node coordination and data transmission. Due to the limited computational power of sensor nodes, implementing complex encryption or intrusion detection systems is often infeasible. This makes the development of lightweight, real-time jamming detection mechanisms critical for maintaining reliable operation in WSN deployments.

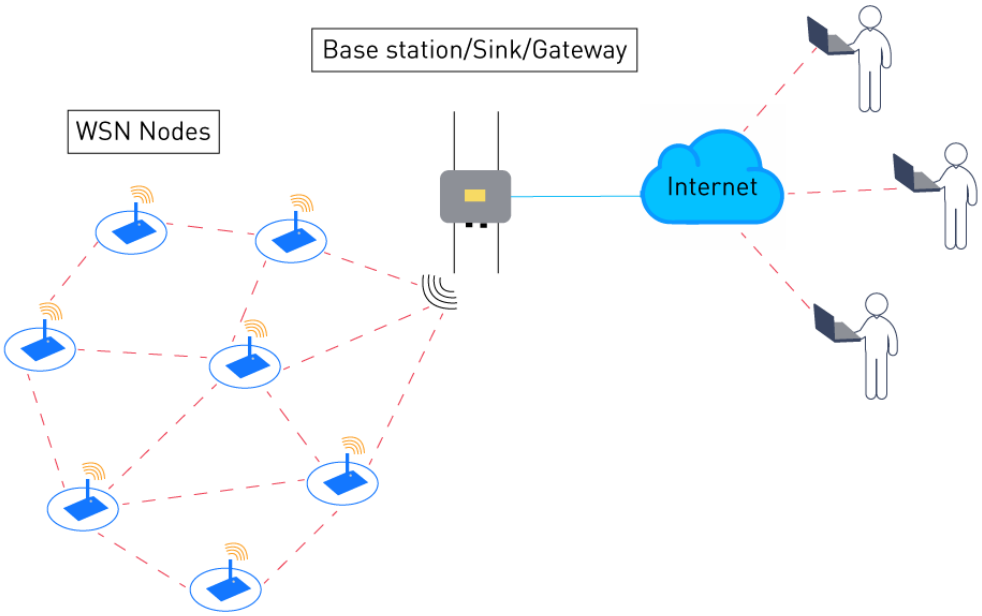


Figure 2.1: Architecture of a Wireless Sensor Network [1]

2.1.2 Internet of Things

The **Internet of Things (IoT)**, as illustrated in Figure 2.2, refers to a global network of interconnected physical objects, commonly referred to as “things”, that are embedded with sensors, actuators, software, and communication modules [18]. These components allow gadgets to gather, send, and process data autonomously, often with little to no human assistance. The scope of IoT spans a wide spectrum of applications, ranging from simple household objects like

smart thermostats and lighting systems to highly complex and specialized industrial tools used in manufacturing, healthcare, agriculture, and environmental monitoring [18].

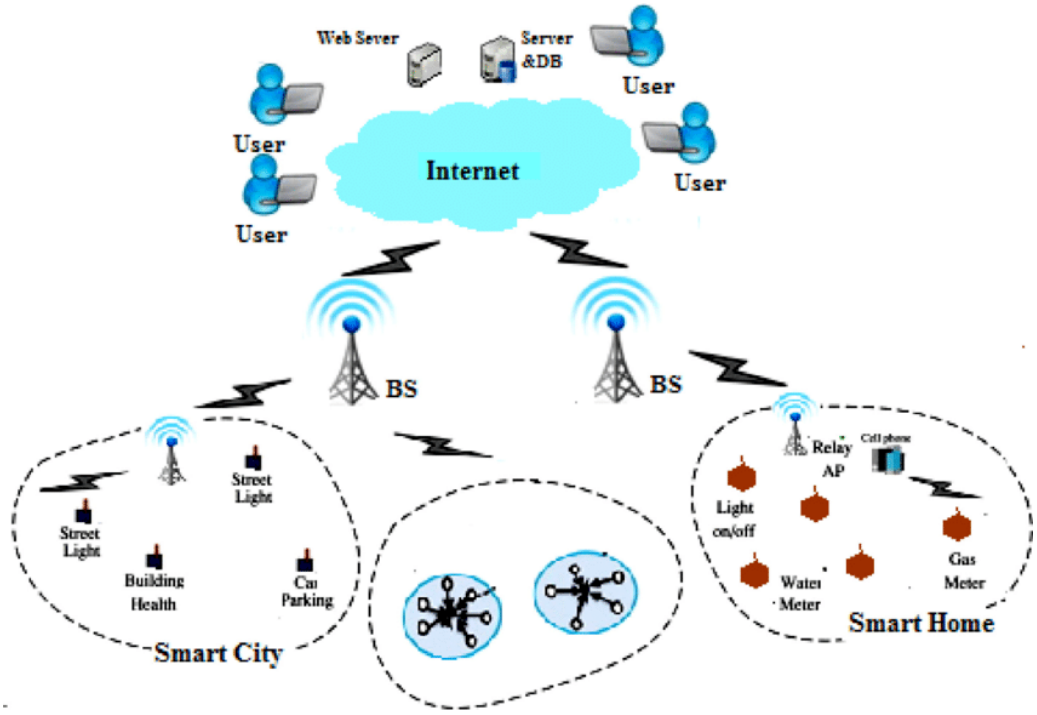


Figure 2.2: IoT Network Architecture [2]

An IoT system typically consists of four parts [8]:

- *Physical-layer sensing devices:* They monitor environmental or system conditions
- *Communication modules:* Enable data exchange over wireless or wired networks
- *Edge or cloud-based platforms:* This is where data is aggregated, processed, and analyzed
- *User interfaces or control systems:* Allow human or machine interaction with the data.

Many IoT devices are designed to be compact and power-efficient, which often results in limited computational capabilities, small memory footprints, and reliance on battery power. These constraints make energy-efficient communication protocols and lightweight computing models essential for their successful operation. In most deployments, wireless communication technologies such as Wi-Fi, Bluetooth, ZigBee, LoRaWAN, and NB-IoT are used to facilitate connectivity [8] [18].

A major limitation of IoT devices stems from their design focus on compactness and power efficiency. As a result, these devices typically possess limited computational capabilities, small memory footprints, and rely heavily on battery-powered operation. Consequently, the adoption of energy-efficient communication protocols and lightweight computing models becomes essential to ensure their long-term functionality and sustainability in real-world deployments.Wireless

communication technologies including Wi-Fi, Bluetooth, ZigBee, LoRaWAN, and NB-IoT are utilized to facilitate connectivity [19] [20].

Significant risks are introduced by the same traits that make IoT devices extremely flexible [21]. Malicious actors find them appealing because of their physical exposure in a variety of settings, dependence on open wireless channels and lack of centralized supervision. Jamming and interference attacks, which target the physical layer to stop devices from sending or receiving data, are among the most disruptive threats. The security, availability, and dependability of IoT systems can be seriously compromised by such attacks.

Ensuring reliable, real-time detection of physical-layer threats has emerged as a major research topic in light of these difficulties.

2.1.3 Jamming Attacks

Jamming is a deliberate form of interference in wireless communication that disrupts the transmission and reception of legitimate signals. By overwhelming the wireless channel with noise or falsified transmissions, an attacker can effectively prevent devices from exchanging data, thereby degrading or entirely halting network functionality [22]. Jamming attacks primarily target the physical layer of the communication stack and are considered a particularly severe threat in wireless networks, especially those deployed in mission-critical and real-time applications such as industrial automation, healthcare monitoring, and military systems.

There are several known types of jamming, including [23] [22]:

- **Constant Jamming:** The attacker emits continuous high-power noise or modulated signals to occupy the wireless channel, effectively preventing legitimate transmissions at all times.
- **Random Jamming:** Interference is transmitted periodically to conserve the attacker's energy while still disrupting communication.
- **Reactive Jamming:** The attacker remains silent until it detects a legitimate transmission and then transmits noise or a fake signal to interfere with it in real-time.
- **Deceptive Jamming:** Rather than just creating noise, this approach mimics valid packets or signals, causing receivers to misinterpret or discard genuine communication.

Jamming is especially dangerous because it can be initiated with inexpensive, widely accessible gear, including software-defined radios (SDRs), which make it easy for attackers to create unique interference patterns [24]. This makes it a highly feasible attack in open environments where physical access or proximity to devices is possible.

The impact of jamming is particularly significant in IoT and WSN installations, which are fre-

quently characterized by resource-constrained, battery-powered devices [25]. These systems usually don't have the processing power to carry out sophisticated cryptographic mitigation or anti-jamming protections. Furthermore, it is hard to tell the difference between intentional jamming, poor signal circumstances, and collisions due to the nature of low-power protocols like those based on ALOHA (like LoRaWAN).

Since jamming symptoms (e.g., increased packet loss, delay, or missed acknowledgments) might be mistaken for harmless interference or network congestion, real-time jamming detection is extremely challenging. This ambiguity often leads to delayed or inaccurate threat identification, which can significantly undermine the reliability and responsiveness of wireless systems, especially in critical IoT and WSN deployments.

2.1.4 LoRaWAN

LoRaWAN (Long Range Wide Area Network) as described in [26] is a low-power, wide-area networking protocol designed for long-range communication between devices in IoT and WSN applications. It operates in unlicensed frequency bands and uses the LoRa physical layer, which employs Chirp Spread Spectrum (CSS) modulation to achieve robustness over long distances with minimal energy consumption.

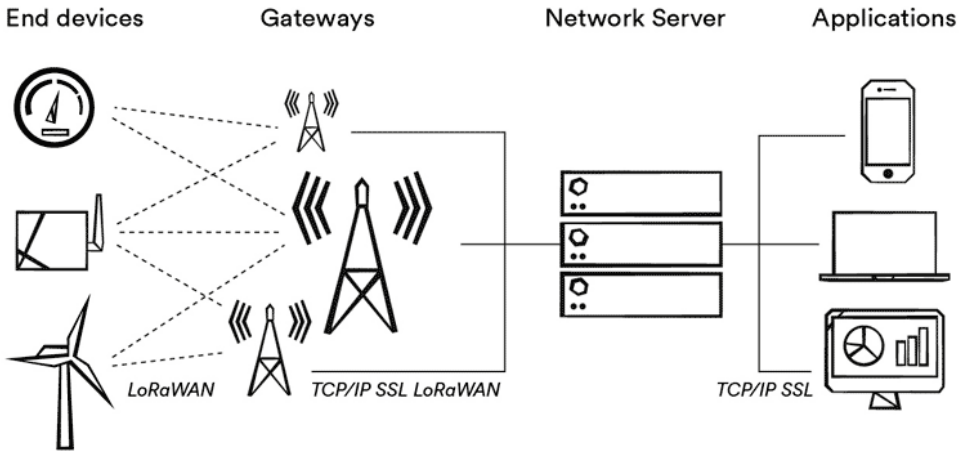


Figure 2.3: LoRaWAN Architecture [3]

LoRaWAN, as shown in Figure 2.3, supports a star topology in which end devices communicate directly with gateways, which then relay the data to a centralized network server. This architecture is particularly well-suited for IoT and Wireless Sensor Network (WSN) deployments where devices are distributed over large areas and require low-power, infrequent communication. Its key features include [26] [27]:

- **Low power consumption**: Enabling multi-year battery life for battery-operated nodes.

- **Long-range communication**: Supporting distances of up to 15 km in rural settings and several kilometers in urban areas.
- **Adaptive Data Rate (ADR)**: Dynamically optimizing transmission power and data rates based on network conditions and distance to gateways.
- **ALOHA-based MAC layer**: A simple medium access scheme that does not require synchronization or coordination between devices but lacks built-in collision avoidance or detection.

Despite its advantages, LoRaWAN's design simplicity introduces several vulnerabilities, particularly at the physical and MAC layers. The use of an uncoordinated ALOHA-based MAC protocol means that packet collisions are common under high network load, and the protocol provides no inherent mechanism for identifying or responding to deliberate interference. This makes LoRaWAN susceptible to physical-layer threats such as jamming, where an attacker can degrade communication by overwhelming the channel with noise or interference[27] [26].

Moreover, LoRaWAN operates in unlicensed spectrum bands (e.g., 868 MHz in Europe, 915 MHz in the U.S.), which are shared with other technologies and devices. This makes it harder to differentiate between unintentional and intentional signal disturbances and raises the possibility of interference.

Given these features, LoRaWAN is a technology that is both useful and underexplored for the creation and assessment of real-time, lightweight jamming detection techniques. Its extensive use in distributed, low-power IoT applications like asset tracking, smart agriculture, and environmental monitoring [28] [27] emphasizes how crucial it is to fix these flaws in order to guarantee dependable and secure system operation.

2.1.5 Fuzzy Logic

Developed by mathematician *Lotfi A. Zadeh* in 1965 through his seminal work on fuzzy sets [29], fuzzy logic emerged as a groundbreaking mathematical framework for processing data with subjective or imprecise boundaries, such as qualitative terms like ”warm weather”, ”high risk”, or ”tall person”. More precisely, instead of using binary logic of true or false, fuzzy logic is a computational method for variable processing that enables reasoning with degrees of truth. Fuzzy logic can function with a continuum of values, unlike traditional systems that need exact, crisp inputs. It excels in real-world scenarios where the data is frequently inaccurate, ambiguous, or incomplete. By mapping verbal concepts such as ”hot,” ”cold,” ”high,” or ”low” to numerical ranges using membership functions, it allows systems to analyze and handle data. In order to arrive at the best logical conclusion given the ambiguity in the input data, fuzzy logic applies heuristic techniques and evaluates all available information in order to solve complicated

situations.

By introducing three key elements: *fuzzy inference rules*, *membership functions*, and *linguistic variables*, this innovative approach fundamentally alters the way systems handle uncertainty. The idea of *linguistic variables*, or variables whose values are expressed in terms of natural language rather than precise numbers, is central to fuzzy logic. For example, a ”temperature” variable might accept values such as ”cold,” ”cool,” ”warm,” or ”hot,” each of which denotes a fuzzy set with precisely defined limits [30].

Membership functions, which provide each potential input value with a degree of belonging between 0 and 1, are used to quantitatively define these linguistic notions. A 25 ° C temperature might be:

- 0.8 ”warm”
- 0.3 ”hot”
- 0.0 ”cold”

This overlapping representation enables seamless transitions between categories, mimicking human intuition in interpreting real-world phenomena.

The true strength of fuzzy logic lies in its rule-based inference system, which employs logical if-then rules to emulate human decision-making. A typical rule might state:

IF traffic is heavy AND weather is rainy, THEN driving speed is low.

Each rule component (e.g., ”heavy traffic” or ”rainy weather”) is precisely quantified through membership functions, where:

- 0 → No membership
- 1 → Full membership
- Intermediate values → Partial membership

The complete fuzzy inference process as described in [31], involves five methodical stages, as shown in Figure 2.4:

1. **Fuzzification**: Transformation of crisp inputs into membership degrees.
2. **Rule Evaluation**: Application of fuzzy operators (min for AND, max for OR) to antecedents.
3. **Implication**: Determination of consequent strength through implication methods (e.g., Mamdani).
4. **Aggregation**: Combination of outputs from all activated rules.
5. **Defuzzification**: Conversion of fuzzy outputs to actionable crisp values.

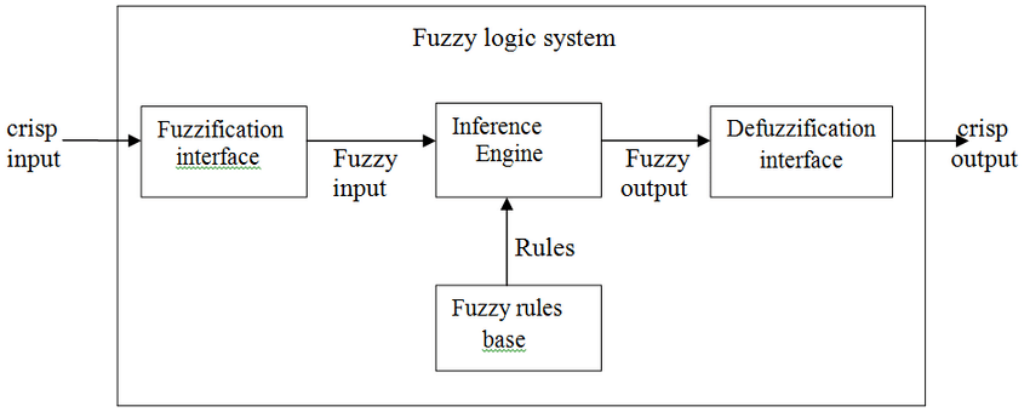


Figure 2.4: Architecture of a fuzzy logic system [4]

Fuzzy logic has proven particularly effective in cybersecurity, where its if-then rules enable efficient and intuitive modeling of security attacks [32]. Due to its interpretability and flexibility, fuzzy logic has clear benefits over other methods, such as decision trees or neural networks, in the detection of network anomalies. Because fuzzy rules and membership functions are transparent, security analysts may quickly modify thresholds or add new attack patterns without having to completely redesign the entire system. This flexibility is essential in dynamic settings where changing threats require small-scale adjustments.

2.1.6 Membership Functions

The Mamdani fuzzy inference system, developed by Ebrahim Mamdani in 1975 [33], was selected for this research due to its demonstrated superiority over alternative approaches (particularly the Sugeno model) in network security and jamming detection applications. The model's principal advantages stem from its unique architecture and operational characteristics that align exceptionally well with the requirements of cybersecurity systems.

Foremost among these advantages is the model's inherently interpretable rule structure, which employs linguistic variables and natural language descriptors that closely parallel human cognitive processes in threat assessment. This transparent architecture offers significant practical benefits over the more mathematically opaque formulations of the Sugeno model. Security domain experts can readily comprehend, verify, and modify the rule base without requiring extensive mathematical training, enabling effective collaboration between cybersecurity professionals and system developers. The system implements this through flexible membership functions that quantify linguistic terms, including [34]:

- **Triangular functions** (defined by center point and width) for simple, computationally efficient representations

- **Trapezoidal functions** (with flat tops and sloping sides) to model stable operational ranges with gradual transitions
- **Gaussian functions** for smooth, naturally distributed phenomena in network traffic patterns
- **Sigmoidal functions** to capture threshold behaviors in attack detection scenarios

The visual interpretability of these functions enables analysts to immediately verify the threat categorization boundaries, guaranteeing that the system's judgment is in line with operational experience.

In our fuzzy logic-based jamming detection system, trapezoidal membership functions (TMFs) are employed, beacause of their mathematical properties and practical advantages in modeling network security threats [35].

A trapezoidal membership function is defined by four parameters **(a, b, c, d)**, which shape its characteristic quadrilateral form as illustrated in Figure 2.5:

- **a**: The point where membership begins ($\mu = 0$)
- **b**: The point where full membership begins ($\mu = 1$)
- **c**: The point where full membership ends ($\mu = 1$)
- **d**: The point where membership ends ($\mu = 0$)

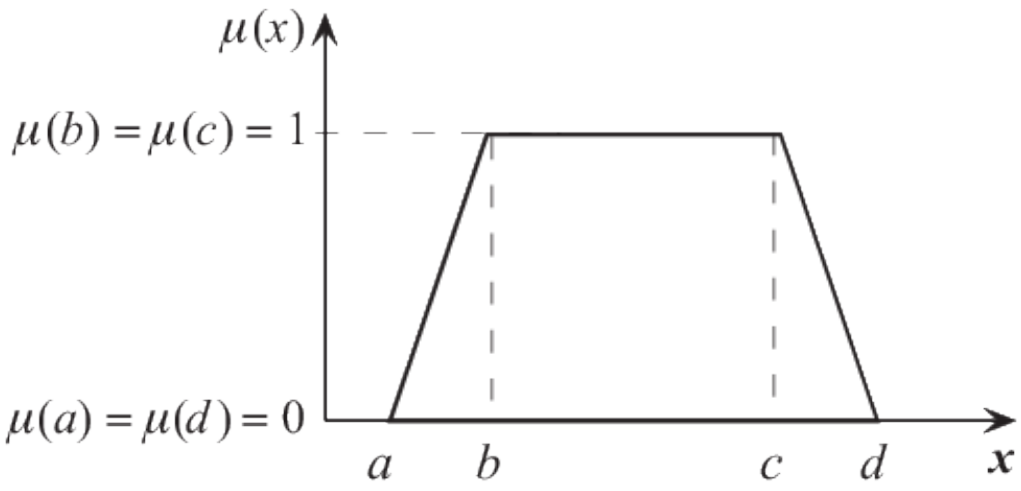


Figure 2.5: Trapezoid-shaped membership function [5]

Mathematically, it is expressed as:

$$\mu(x) = \begin{cases} 0, & x \leq a \\ \frac{x-a}{b-a}, & a < x < b \\ 1, & b \leq x \leq c \\ \frac{d-x}{d-c}, & c < x < d \\ 0, & x \geq d \end{cases} \tag{2.1}$$

This structure creates a *flat top (between b and c)* and *sloping sides (a-b and c-d)*, allowing smooth transitions between membership levels.

The intrinsic ambiguity of attack signatures frequently makes it difficult to accurately classify threats in the field of network security. Because malicious behavior often takes the form of a spectrum of anomalies rather than absolute states, traditional binary thresholds are unable to capture the graded nature of jamming assaults. The best mathematical foundation for modeling both the definite zones of threat categorization and the transitional areas where uncertainty predominates is provided by the four-parameter structure of trapezoidal membership functions [36] . Security systems can make complex, real-time choices that take into account both observed network circumstances and expert subject knowledge thanks to trapezoidal functions, which combine interpretability and computing efficiency. Their sloping edges allow for the inherent variation seen in normal traffic patterns, and their level plateaus provide distinct thresholds for actionable alarms. This introduction examines the reasons for the popularity of trapezoidal functions in fuzzy logic-based jamming detection systems, which strike a balance between mathematical precision and real-world security needs.

2.2 Related Work

This section reviews existing research on security threats in Wireless Sensor Networks (WSNs), Internet of Things (IoT) and LoRaWAN focusing on various attack types, detection mechanisms, and mitigation strategies. In addition, it explores how fuzzy logic has been applied as a lightweight and interpretable approach to detect anomalies in wireless systems.

The research [37] examines major attacks on Wireless Sensor Networks (WSNs), such as wormhole, jamming, selective forwarding, sinkhole, and Sybil attacks, and proposes countermeasures. The researchers' findings include the presentation of detection and prevention techniques, such as statistical analysis, directional antenna usage, and trust-based methods. Additionally, they identify challenges in wormhole and sinkhole attacks due to the dynamic topology of WSNs. The need for additional resources and specialized hardware complicates the application of these solutions, increasing overall costs.

Another study expands the focus to IoT networks [38], categorizing them into four main types: physical, network, software, and cryptographic attacks. It concludes by identifying the most dangerous attacks in each category. Suggested countermeasures include monitoring verification for detecting malicious nodes and node authentication techniques to mitigate sinkhole attacks. However, these approaches face limitations due to the low computational power and energy constraints of IoT devices.

Jamming attacks are one of the most significant threats to IoT networks and require highly efficient detection systems. The following study [25] creates a real-time jamming detection system for Wi-Fi Internet of Things networks in this context. The mechanism achieves 99% detection accuracy with low computational requirements, making it suitable for cost-effective IoT devices. Experimental results demonstrate a significant reduction in network throughput and packet delivery rate during jamming attacks. However, low-power interference negatively affects accuracy, and the system requires adaptation to topology changes or varying network conditions.

Another approach [4] explores jamming detection and mitigation in LoRaWAN networks, leveraging machine learning and cloud services for improved accuracy. A testbed was implemented where jamming attacks were simulated, and the collected data was used to train machine learning algorithms, such as LSTM Autoencoders, to detect jamming with high accuracy. However, a limitation of the study is that the experiments were conducted in a controlled environment. In real-world scenarios, changes in network topology and dynamic network behavior may affect performance.

Building on the efforts to detect jamming in LoRaWAN networks and enhance security during the LoRa node connection procedure, the thesis [39] presents an Intrusion Detection System (LIDS). More precisely, it describes experimental tests conducted in a controlled testbed environment using the LoRaWAN protocol. The researchers proposed two detection algorithms, Kullback-Leibler Divergence (KLD) and Hamming Distance (HD). KLD achieved 98% detection accuracy with a 5% false positive rate (FP). HD achieved 88% detection accuracy with a similar FP rate. Overall, KLD-based LIDS outperforms HD in general accuracy. However, limitations include the fact that experiments were conducted in a controlled environment with LoRa nodes placed at short distances from each other. Additionally, the lack of large-scale applications and limited dataset size prevents the generalization of results.

The authors [36] propose a Fuzzy Logic-based Intrusion Detection System (IDS) for detecting jamming attacks in Wireless Mesh IoT Networks, aiming to provide an intelligent, lightweight, and distributed solution. Their model uses combinations of metrics such as ETX, Retransmissions, PDPT, and PDR as inputs to a Mamdani-type fuzzy inference system to compute a Jamming Index (JI). The main contribution lies in evaluating five different input combinations to

identify which yield the best detection performance, with extensive experimentation conducted in Contiki OS using the Cooja simulator across 48 different jammer positions. The results show that using Retransmissions in combination with ETX or PDPT leads to high accuracy (up to 95%) and effective detection under various network topologies. However, a limitation of the study is its reliance on simulated environments with a static node grid and a single jammer type (a proactive deceptive jammer). Real-world deployments could introduce additional challenges such as dynamic topologies, mobility, environmental interference, and multiple/joint attack types, which were not explored in this work.

The researchers [40] developed a jamming attack mitigation approach for LoRa networks, leveraging temporal and spatial variations of jamming signals. The method utilizes multiple gateways to recover signals affected by strong interference. The study found that the system improved the packet reception rate (PRR) by up to 83.91 times, while reducing the energy consumption per packet by up to 115.65 times compared to standard LoRa operation in outdoor experimental tests. However, further evaluation revealed that system efficiency decreases in more complex scenarios, such as cases where the jammer is continuously moving.

In addition, another study [41] in order to identify targeted interference attacks in NB-IoT networks at the User Equipment (UE) level, the authors suggest a statistical anomaly detector. To differentiate intentional jamming from unintentional interference, the technique tracks subframe loss rates in the downlink channel. The findings of the simulation demonstrate accurate attack detection with adjustable false positive rates, enabling a trade-off between false alarms and detection precision. The restrictions of their work were that they evaluated solely in simulated environments (Matlab) and did not detect interference on synchronization channels.

Michael Savva's Ph.D. dissertation [42], from the University of Cyprus, proposes using network-layer indicators such as Expected Transmission Count (ETX) and Retransmissions in a Fuzzy Logic Intrusion Detection System (FLIDS) to effectively identify jamming attacks in IoT networks. These inputs are transformed into a Jamming Indicator (JI) by fuzzy logic, aiding in the detection of jamming attacks. The experimental results demonstrate that FLIDS achieved high detection accuracy (over 95%) for various types of jamming attacks, including deceptive, reactive, and constant jammers. The system showed low execution time, reduced CPU and memory usage, and real-time attack detection. However, a limitation of this work was that it performed somewhat worse (around 90%) against deceptive jammers that mimic real traffic. Additionally, the method was only evaluated in static IoT networks.

The authors [43] analyze Energy Depletion Attacks (EDAs) in LoRaWAN networks, which aim to drain the battery life of IoT sensors, disrupting network operations and increasing maintenance costs. The paper examines energy consumption models, classifies LoRaWAN attacks and describes different attack types according to how likely they are to consume energy. The find-

ings demonstrate how several Denial-of-Service (DoS) attacks, such as replay, sinkhole, and jammer attacks, lead to energy depletion. Furthermore, the paper also examines the effects of EDAs on the MCU, transmission (TX), and reception (RX) states of LoRaWAN devices and offers an emulation-based characterisation of EDAs. Due to a lack of actual data, several attack classes lack accurate energy consumption metrics.

The authors of this research [44] introduce the Number of Jammed Slots (NJS) metric for identifying proactive and reactive jammers in IoT networks, using MAC-layer status updates gathered by a central node. This technique surpasses current methods, identifying jammers four times quicker, increasing accuracy by 33%, and eliminating the need for specialist gear. It depends on centralized data collecting, and might not be able to withstand adaptive jammers.

Examining detection methodologies, placement tactics, security risks, and validation procedures, the authors [45] examine Intrusion Detection Systems (IDS) for the Internet of Things. They illustrate the advantages and disadvantages of each of the four IDS techniques they classify: signature-based, anomaly-based, specification-based, and hybrid. Key issues are also identified in the report, including protocol-specific security flaws, multi-hop network topologies, and resource limitations in IoT devices. Despite offering a thorough taxonomy of IDS solutions for the Internet of Things, the survey points out that there are few standardized validation frameworks and little real-world testing, which makes it challenging to evaluate various detection techniques.

This study [46] suggests an anomaly detection technique based on machine learning to detect manipulated radio-frequency signals in LoRa networks. They use Principal Component Analysis (PCA), Autoencoder, Variational Autoencoder, Isolation Forest, and Local Outlier Factor on image-based representations of frequency signals.When these techniques were tested on their dataset, which included more than 26,000 photos from actual studies, Local Outlier Factor had the best accuracy (97.78%). Nevertheless, the system was only tested in controlled settings, hasn't been assessed against actual network dynamics, and could need to be further modified to withstand replay or jamming attempts.

Lastly, Bhattacharjee and Begum [47] survey the use of fuzzy logic techniques for Intrusion Detection Systems (IDS) across different network environments. They talk about how fuzzy logic provides an efficient way to distinguish between typical and anomalous network activities because of its ability in managing ambiguity, uncertainty, and imprecise thinking. The study provides a thorough description of IDS types, components, and limits in addition to classifying network attacks (such as DoS, probing, R2L, and U2R). The ability of fuzzy rule-based systems to enhance anomaly detection, smooth decision boundaries, and adjust to changing threats is highlighted. The authors point out that although fuzzy logic improves flexibility and detection accuracy, problems with rule creation, optimization, and real-time deployment still exist. The

study's overall findings highlight the potential of fuzzy approaches in creating more effective and flexible intrusion detection systems for network environments that are becoming more complex and dynamic.

3 Chapter 3

Methodology and Implementation

This chapter outlines the dataset and methodology employed for detecting jamming attacks in a LoRaWAN network. The dataset consists of labeled transmissions collected from a real-world testbed, capturing both normal and jamming conditions. Key physical-layer features such as Received Signal Strength Indicator (RSSI) and Signal-to-Noise Ratio (SNR) were extracted for analysis.

The fuzzy inference system utilizes input variables derived from the physical-layer metrics to classify transmission conditions as either normal or jammed. Membership functions and fuzzy rules were carefully crafted to model the uncertainty and variability inherent in wireless signal behavior. The resulting system produces a Jamming Confidence Score, enabling lightweight, interpretable, and adaptive intrusion detection suitable for deployment on constrained IoT and WSN devices.

All experimental procedures, including dataset preprocessing, fuzzy model construction, and system evaluation, are described in detail in the sections that follow. Figures and tables are provided where appropriate to illustrate key implementation steps and summarize performance outcomes.

3.1 Dataset Description

The experimental analysis utilized a comprehensive dataset comprising 31,919 timestamped and labeled samples collected from a controlled LoRaWAN testbed subjected to reactive jamming attacks. The data capture window spanned 2 hours and 43 minutes of continuous operation from 14:16 to 16:59 on February 8, 2023. Each sample in the dataset represents a complete LoRaWAN transmission and has the following key attributes:

- **Temporal:** Local Time (minute-level precision)
- **Device:** Device Name, deveui (5 unique motes)
- **Physical layer:** Freq[Hz], BW(kHz), SF, coderate
- **Signal metrics:** RSSI(dBm), snrSNR(dB)
- **Environmental**: Temperature (F), Humidity (%)
- **Network:** fcnt (frame counter)

- **Jamming Label:** -1 = Jamming and 1 = Normal (binary classification)

A very notable fact about the dataset is that it exhibits severe class imbalance:

- Jamming instances: 408 (1.28%)
- Normal operation: 31,511 (98.72%)

The dataset exhibits extreme class imbalance, with jamming events ($n = 408$, 1.28%) being approximately 77 times less frequent than normal operation samples ($n = 31,511$, 98.72%). This distribution reflects real-world conditions, where attacks are rare anomalies embedded in predominantly normal network traffic.

After preprocessing the dataset, we observed notable differences in physical-layer signal characteristics between normal and jamming conditions. These differences are quantitatively summarized in Table 3.1, which presents descriptive statistics for the Received Signal Strength Indicator (RSSI) and Signal-to-Noise Ratio (SNR), and are further illustrated in Figure 3.1 through box plots that highlight distributional patterns and variability.

Category	RSSI_min	RSSI_max	RSSI_mean	RSSI_std	SNR_min	SNR_max	SNR_mean	SNR_std
No Jamming	-111	-54	-69.37	5.41	-1.0	15.5	10.94	1.71
Jamming	-96	-39	-65.74	7.89	-3.8	14.5	10.89	1.85

Table 3.1: Statistical Summary of Signal Characteristics by Category

As shown in both Table 3.1 and Figure 3.1, we computed the minimum, maximum, mean, and standard deviation for RSSI and SNR under both scenarios. Jamming conditions exhibited a higher variance in RSSI ($\sigma = 7.89$ vs. $\sigma = 5.41$) and a higher average RSSI (-65.74 dBm vs. -69.37 dBm), indicating possible signal amplification during attacks. While the mean SNR values were nearly identical between the two classes (10.89 dB vs. 10.94 dB), the jamming class showed a lower minimum SNR (-3.8 dB vs. -1.0 dB) and a slightly higher standard deviation (1.85 vs. 1.71), suggesting more unpredictable signal degradation during jamming episodes.

Furthermore, the RSSI range under jamming conditions (-96 to -39 dBm) was narrower than that observed during normal operation (-111 to -54 dBm), potentially due to power constraints or environmental limitations affecting the jammer's signal variability.

These statistical differences demonstrate that jamming attacks induce measurable changes in physical-layer signals. In particular, the increased variation in both RSSI and SNR during jamming suggests that these signal fluctuations can serve as reliable indicators for identifying attacks using detection algorithms.

In addition to RSSI and SNR, the Packet Loss Rate (PLR) was examined as a supplementary indicator of network performance under normal and jamming conditions. PLR measures the percentage of expected but undelivered packets, making it a valuable metric for assessing trans-

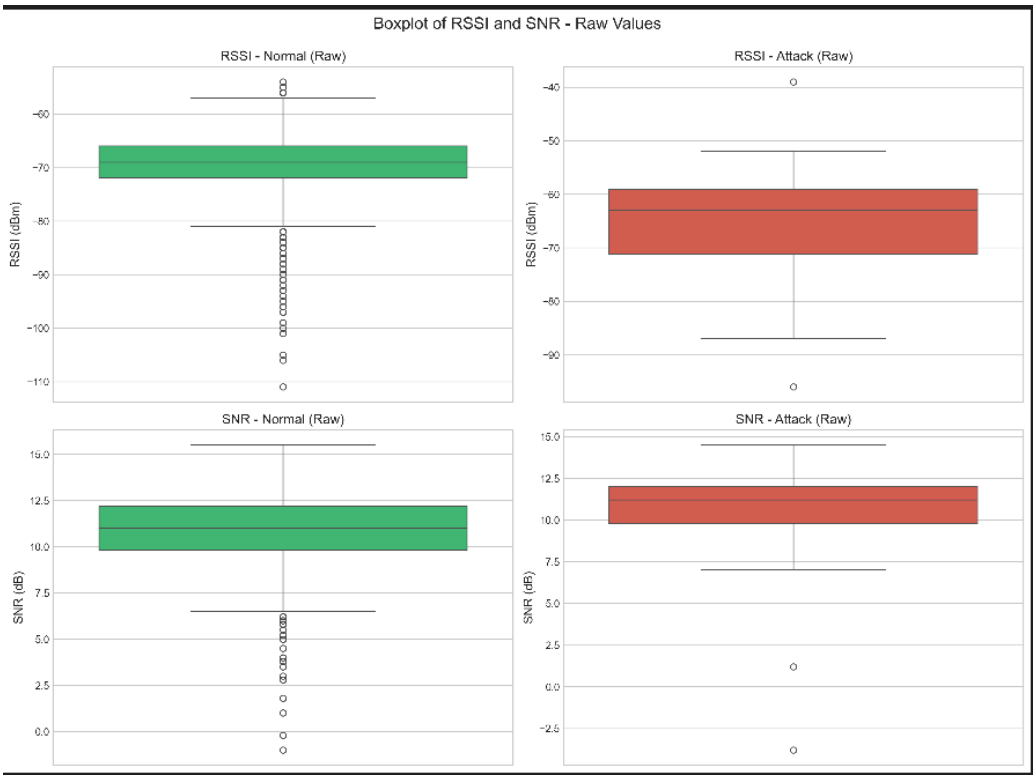


Figure 3.1: Box plots of RSSI and SNR under normal and jamming conditions

mission reliability. Given that jamming directly affects a device's ability to successfully transmit packets, PLR is expected to increase significantly during jamming events.

We computed the PLR for each one of the five motes in the dataset separately under both normal and jamming conditions. The distribution of PLR values across all devices is visualized in Figure 3.2 and Figure 3.3, which show box plots highlighting the spread and central tendencies under both scenarios. As seen, jamming leads to an upward shift in both median and maximum PLR values across all motes, suggesting a consistent increase in packet loss due to interference.

Table 3.2 summarizes the descriptive statistics of PLR per device, reporting minimum, maximum, mean, and standard deviation under both normal and jamming conditions.

Device Name	**Normal**				**Jamming**			
	Min	**Max**	**Mean**	**Std**	**Min**	**Max**	**Mean**	**Std**
Mote01	0.000	0.833	0.2171	0.2814	0.000	0.800	0.3235	0.3280
Mote02	0.000	0.889	0.2147	0.2782	0.000	0.833	0.3051	0.3189
Mote03	0.000	0.857	0.2171	0.2800	0.000	0.857	0.3213	0.3195
Mote04	0.000	0.833	0.2124	0.2783	0.000	0.889	0.3364	0.3137
Mote05	0.000	0.857	0.2172	0.2799	0.000	0.833	0.3233	0.3102

Table 3.2: Statistical Summary of Packet Loss Rate (PLR) by Device and Condition

As shown in Table 3.2, Figure 3.2 and Figure 3.3 , all devices exhibit higher average PLR and greater variance under jamming conditions compared to normal ones. For example, Mote04 has the highest mean PLR under jamming (0.336), reflecting the increased likelihood of disrupted transmissions. In contrast, PLR under normal operation remains relatively low and consistent across devices (mean values ≈ 0.21), demonstrating stable communication in the absence of interference.

These findings confirm that PLR is a sensitive and discriminative indicator of jamming activity. The increased average and variability in PLR during attacks suggest that it can be reliably used in conjunction with either RSSI or SNR as input features for anomaly detection models, such as the fuzzy logic-based approach implemented in this study.

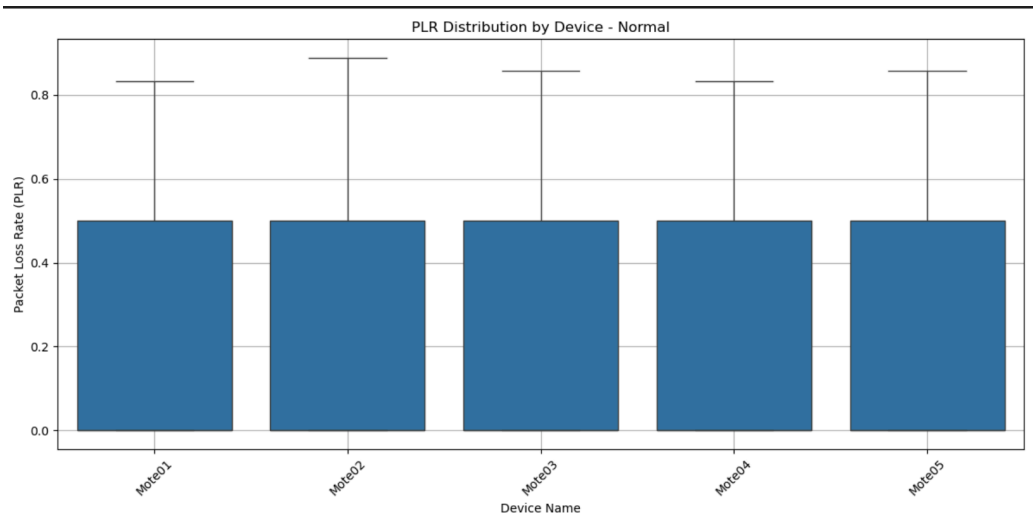


Figure 3.2: Box plots of Packet Loss Rate (PLR) under normal conditions

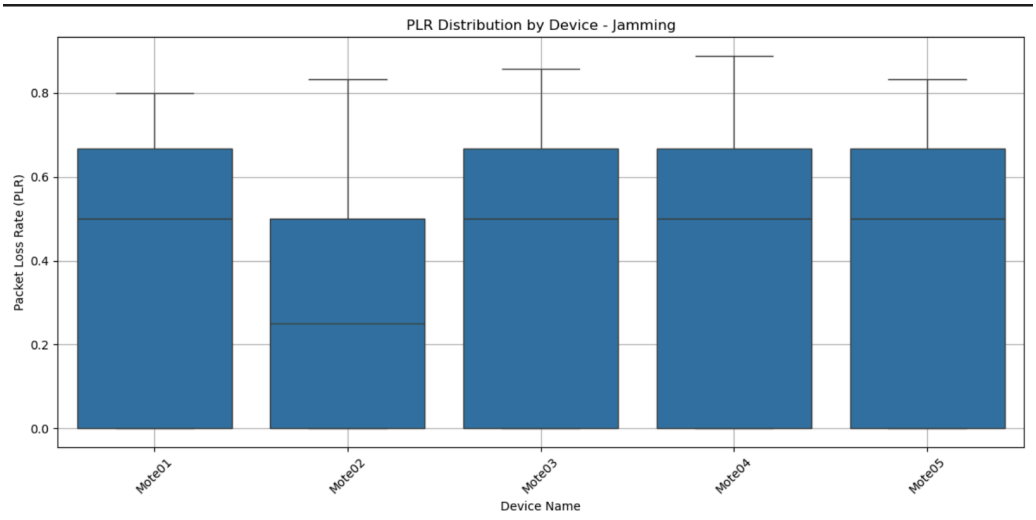


Figure 3.3: Box plots of Packet Loss Rate (PLR) under jamming conditions

3.1.1 Metrics

This subsection briefly describes the physical-layer and link-layer metrics used as input features in the fuzzy inference models for jamming detection: RSSI, SNR, and PLR [48] [36].

Received Signal Strength Indicator (RSSI) is a measure of the power level received by the radio, expressed in decibels-milliwatts (dBm). It provides an indication of signal strength but is susceptible to non-malicious environmental factors such as transmission distance, physical obstructions, and variations in legitimate transmission power. RSSI is widely supported on wireless communication devices and serves as a readily available signal quality indicator.

Signal-to-Noise Ratio (SNR) quantifies the ratio between the received signal power and the background noise, measured in decibels (dB). It reflects the clarity or quality of a signal, where higher values suggest cleaner reception and better communication conditions. Unlike RSSI, SNR directly incorporates channel interference and noise, making it a more precise measure of signal fidelity.

Packet Loss Rate (PLR) is a normalized metric that represents the proportion of packets that are lost during transmission relative to those sent. It provides a direct measure of link-layer reliability. Elevated PLR values typically indicate transmission degradation, which is characteristic of jamming scenarios. As such, PLR is especially effective in identifying disruptive behavior in wireless networks.

3.2 Model's Implementation

3.2.1 Fuzzy Inference Model: RSSI and SNR Combination

In this configuration, the fuzzy logic model uses Received Signal Strength Indicator (RSSI) and Signal-to-Noise Ratio (SNR) as input features to estimate the likelihood of jamming. Both metrics provide essential information on signal integrity and communication quality.

By combining RSSI and SNR, the system leverages complementary indicators of abnormal physical-layer behavior. The fuzzy inference system, as illustrated in Figure 3.4, produces a Jamming Index (JI), a continuous score between 0 and 1, where higher values indicate greater likelihood of jamming activity.

This system was developed in Python, with MATLAB used for membership function design and visualization. The membership functions for RSSI and SNR were informed by empirical patterns observed in the dataset, along with reference values commonly found in LoRaWAN literature. Table 3.3 summarizes the trapezoidal parameters used for each fuzzy set.

Figures 3.5, 3.6, and 3.7 illustrate the defined membership functions for RSSI, SNR, and Jam-

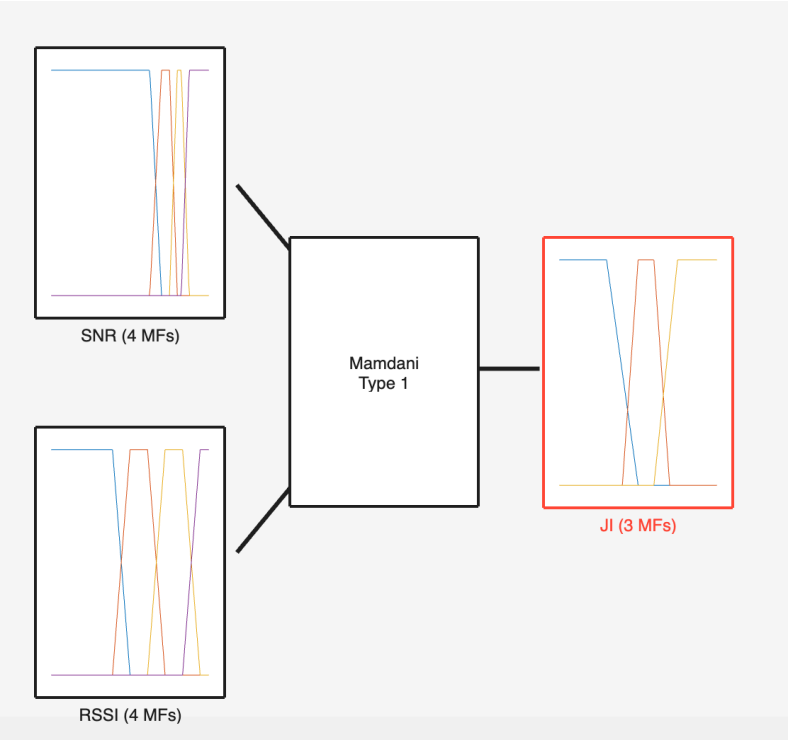


Figure 3.4: Structure of the Mamdani Fuzzy Inference System using RSSI and SNR as inputs and Jamming Index (JI) as output

ming Index respectively.

Figure 3.5 shows the RSSI membership function, partitioned into *Very Weak*, *Weak*, *Moderate*, and *Strong*. Figure 3.6 displays the corresponding SNR fuzzy sets: *Very Low*, *Low*, *Moderate*, and *High*. The output Jamming Index is defined using three fuzzy sets: *Low*, *Medium*, and *High*, providing a smooth and continuous interpretation of the jamming likelihood.

Given that RSSI and SNR each have four fuzzy sets, and the fuzzy system maps every possible combination of RSSI and SNR to a JI output, a total of $4 \times 4 = 16$ fuzzy rules are required for this configuration.

3.2.2 Fuzzy Inference Model: PLR and RSSI Combination

To design a lightweight and interpretable jamming detection system, a fuzzy logic-based model was implemented using Packet Loss Rate (PLR) and Received Signal Strength Indicator (RSSI) as input features. The architecture of the fuzzy inference system, which integrates these input features to compute a continuous Jamming Index (JI), is illustrated in Figure 3.11.

The fuzzy system uses linguistic variables to model the imprecise nature of wireless communication. By combining PLR and RSSI, the system can reason under uncertainty and generate a Jamming Index (JI). JI is a continuous-valued score between 0 and 1 that reflects the likelihood

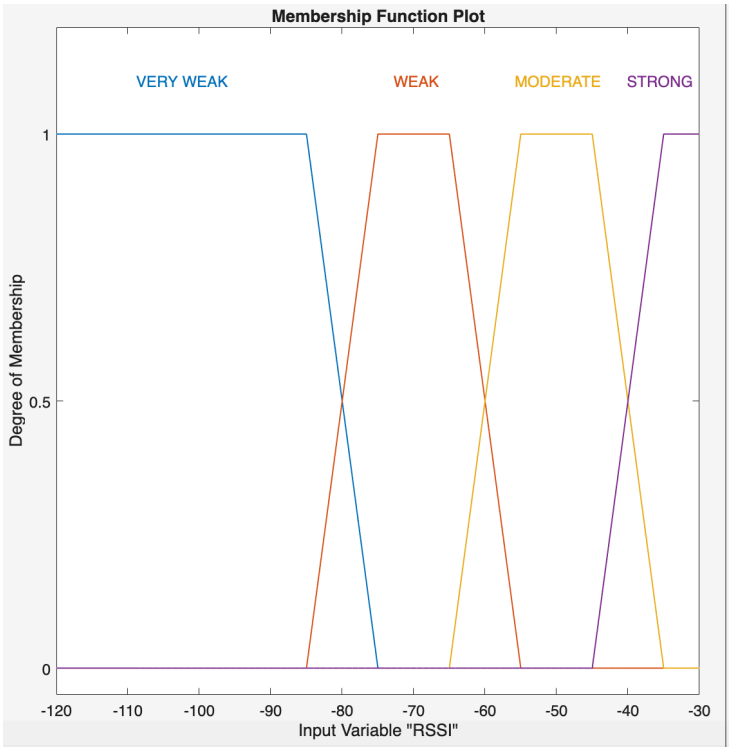


Figure 3.5: The Trapezoidal Membership Function Plot for RSSI

of a jamming event occurring. A value closer to 1 indicates a high probability of jamming, while a value closer to 0 indicates a normal event.

The fuzzy inference system was developed in Python, while MATLAB was used to design and visualize the membership functions. Figures 3.9, 3.18, and 3.10 show the membership function plots for RSSI, PLR, and JI respectively.

Table 3.4 summarizes the parameters used to define the trapezoidal membership functions for all three variables. These ranges were selected based on a statistical distribution analysis of the dataset and by consulting published studies on the characteristics of the LoRaWAN network, particularly for the RSSI metric. The range for the packet loss rate (PLR) was established at [0, 1] as it represents a normalized ratio of lost packets over total transmitted packets, which by definition varies between 0 (no loss) and 1 (complete loss).

Since the RSSI input has four fuzzy sets and PLR has three fuzzy sets, the total number of fuzzy rules required to cover all possible input combinations in this model is $4 \times 3 = 12$.

3.2.3 Fuzzy Inference Model: PLR and SNR Combination

Another fuzzy logic-based model was implemented using Packet Loss Rate (PLR) and Signal-to-Noise Ratio (SNR) as input features.

The architecture of this fuzzy inference system, which integrates PLR and SNR to compute a

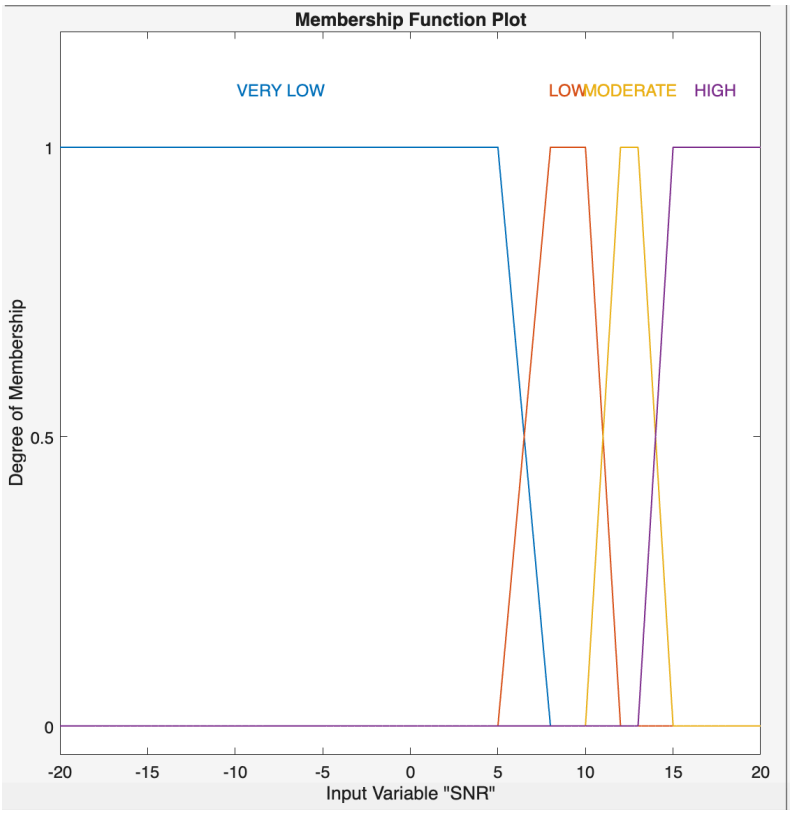


Figure 3.6: The Trapezoidal Membership Function Plot for SNR

continuous Jamming Index (JI), is illustrated in Figure 3.12. As with previous models, JI is a continuous score in the range [0, 1], where values close to 1 indicate a high likelihood of jamming, and values near 0 suggest normal network operation.

The fuzzy inference system was again developed in Python, while MATLAB was used for visualization. Figures 3.14, 3.18, and 3.13 show the membership functions defined for SNR, PLR, and the Jamming Index, respectively.

Table 3.5 summarizes the trapezoidal membership function parameters for all three variables. These ranges were selected based on statistical distribution analysis of the dataset and reference values reported in the literature for typical LoRaWAN communication conditions. The PLR input remains normalized in the range [0, 1], representing the proportion of lost packets.

The SNR membership function, shown in Figure 3.14, defines four fuzzy sets: Very Low, Low, Moderate, and High. The PLR input retains its fuzzy partitioning as shown and mentioned previously in Figure 3.18. The Jamming Index is similarly defined in Low, Medium, and High fuzzy sets in Figure 3.13, allowing for consistent interpretation across models.

Since the SNR input has four fuzzy sets and PLR has three fuzzy sets, the total number of fuzzy rules required to cover all possible input combinations in this model is $4 \times 3 = 12$.

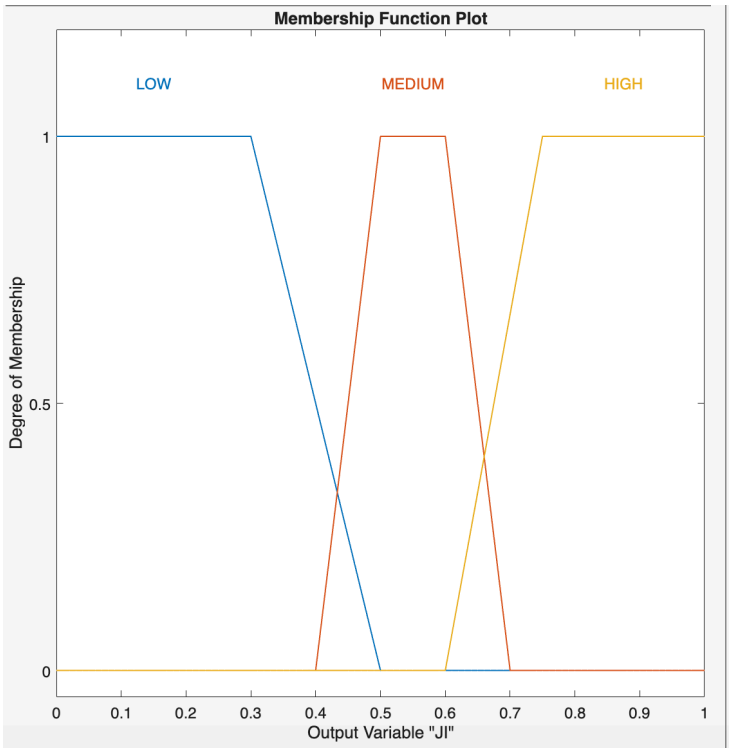


Figure 3.7: The Trapezoidal Membership Function Plot for Jamming Index (JI)

3.2.4 Fuzzy Inference Model: RSSI, SNR, and PLR Combination

To develop a more robust and accurate fuzzy logic-based jamming detection system, this model incorporates three input features: Received Signal Strength Indicator (RSSI), Signal-to-Noise Ratio (SNR), and Packet Loss Rate (PLR).

The fuzzy inference system (FIS) combines these inputs to compute a continuous-valued output, the Jamming Index (JI), ranging from 0 (no jamming) to 1 (high likelihood of jamming). This architecture is illustrated in Figure 3.15.

The system was developed in Python, and the membership functions were designed and visualized in MATLAB. The trapezoidal membership functions for each variable were defined to reflect empirical patterns in the dataset and common values reported in LoRaWAN deployments.

Figures 3.9, 3.16, and 3.18 depict the membership function plots for the input variables, and Figure 3.17 shows the corresponding output membership function for JI. These fuzzy sets were chosen to capture realistic variability in wireless communication environments and to enable flexible classification boundaries. The use of PLR alongside RSSI and SNR addresses some of the challenges that exist in prior models.

Since the RSSI input has four fuzzy sets, SNR has four fuzzy sets, and PLR has three fuzzy sets, the total number of fuzzy rules required to cover all possible input combinations in this model

Variable	Set	a	b	c	d
RSSI (dBm)	Very Weak	-120	-120	-85	-75
	Weak	-85	-75	-65	-55
	Moderate	-65	-55	-45	-35
	Strong	-45	-35	-30	-30
SNR (dB)	Very Low	-20	-20	5	8
	Low	5	8	10	12
	Moderate	10	12	13	15
	High	13	15	20	20
Jamming Index (JI)	Low	0.0	0.0	0.3	0.5
	Medium	0.4	0.5	0.6	0.7
	High	0.6	0.75	1.0	1.0

Table 3.3: Trapezoidal membership function parameters for RSSI, SNR, and Jamming Index

Variable	Set	a	b	c	d
RSSI (dBm)	Very Weak	-120	-120	-90	-80
	Weak	-90	-80	-70	-60
	Moderate	-70	-60	-50	-40
	Strong	-50	-40	-30	-30
PLR	Low	0.0	0.0	0.1	0.2
	Moderate	0.15	0.25	0.35	0.45
	High	0.4	0.5	1.0	1.0
Jamming Index (JI)	Low	0.0	0.0	0.2	0.4
	Medium	0.3	0.4	0.6	0.7
	High	0.6	0.8	1.0	1.0

Table 3.4: Trapezoidal membership function parameters for RSSI, PLR and Jamming Index

is $4 \times 4 \times 3 = 48$.

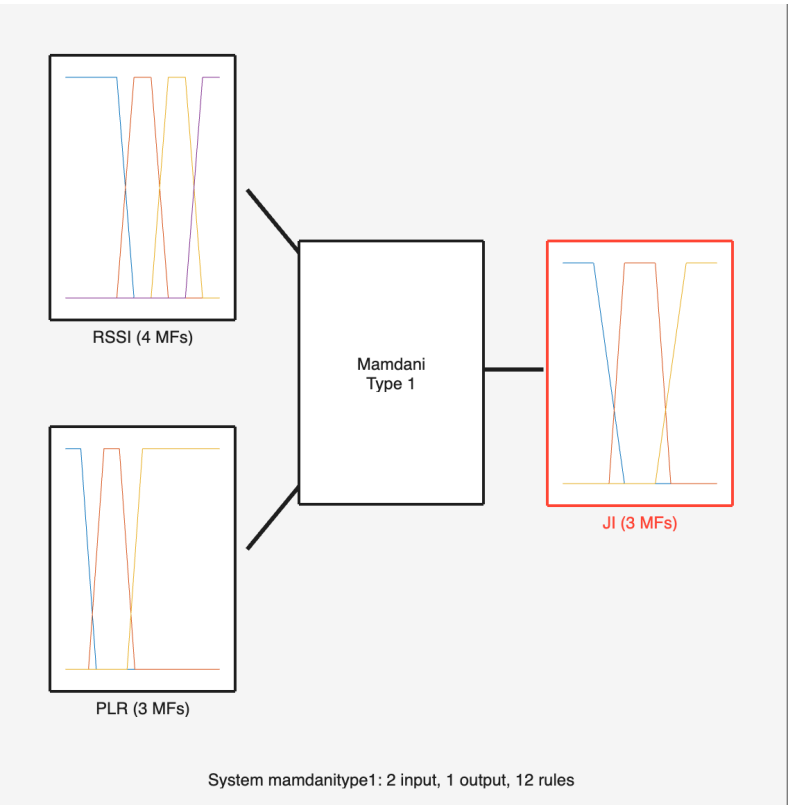


Figure 3.8: Structure of the Mamdani Fuzzy Inference System using RSSI and PLR as inputs and Jamming Index (JI) as output

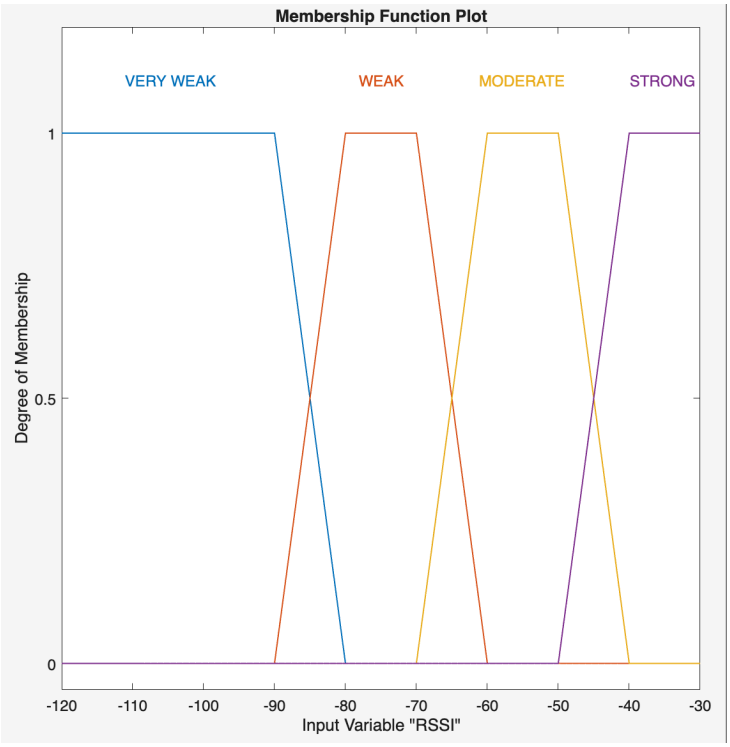


Figure 3.9: The Trapezoidal Membership Function Plot for RSSI

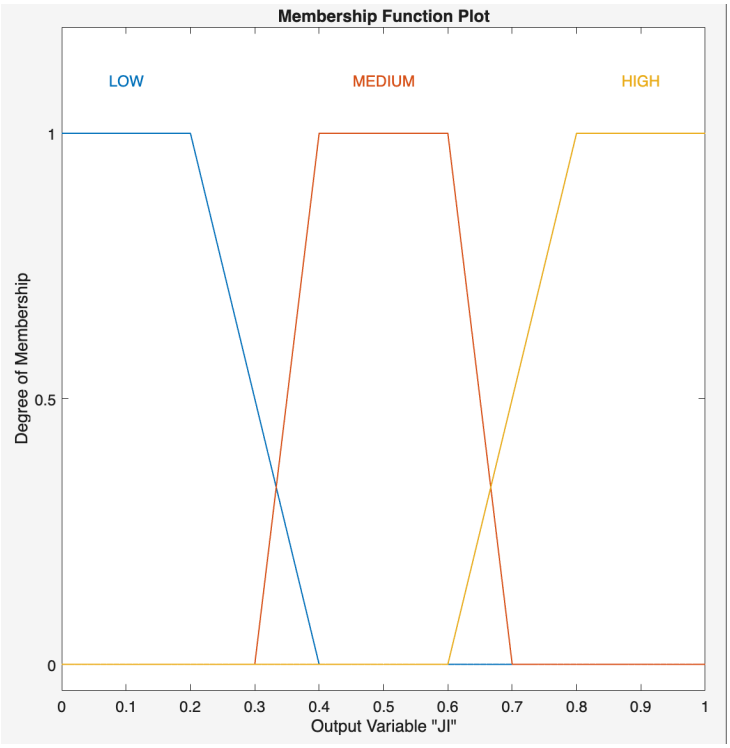


Figure 3.10: The Trapezoidal Membership Function Plot for Jamming Index (JI)

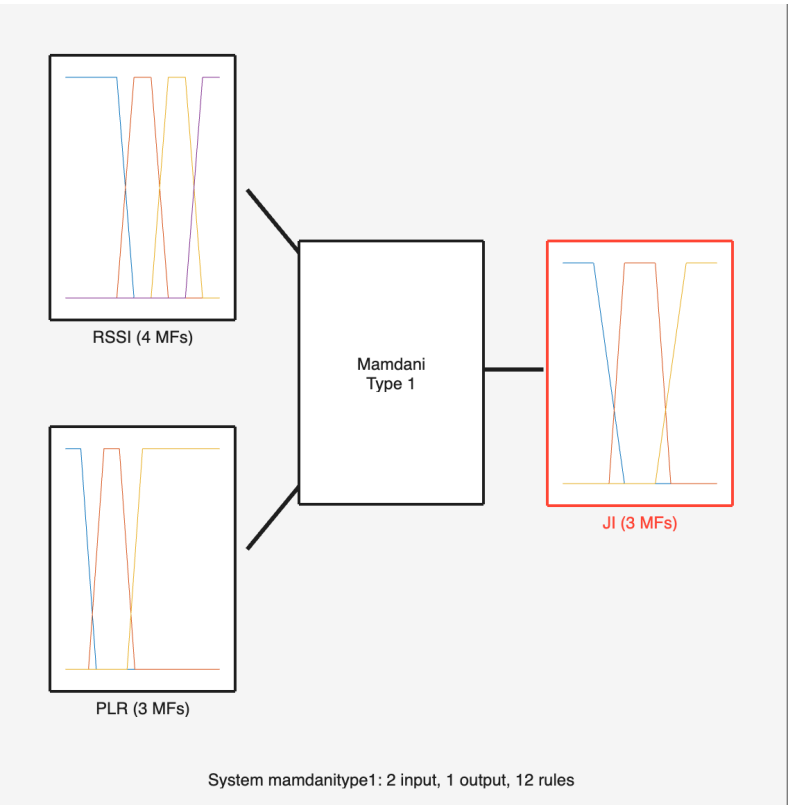


Figure 3.11: Structure of the Mamdani Fuzzy Inference System using RSSI and PLR as inputs and Jamming Index (JI) as output

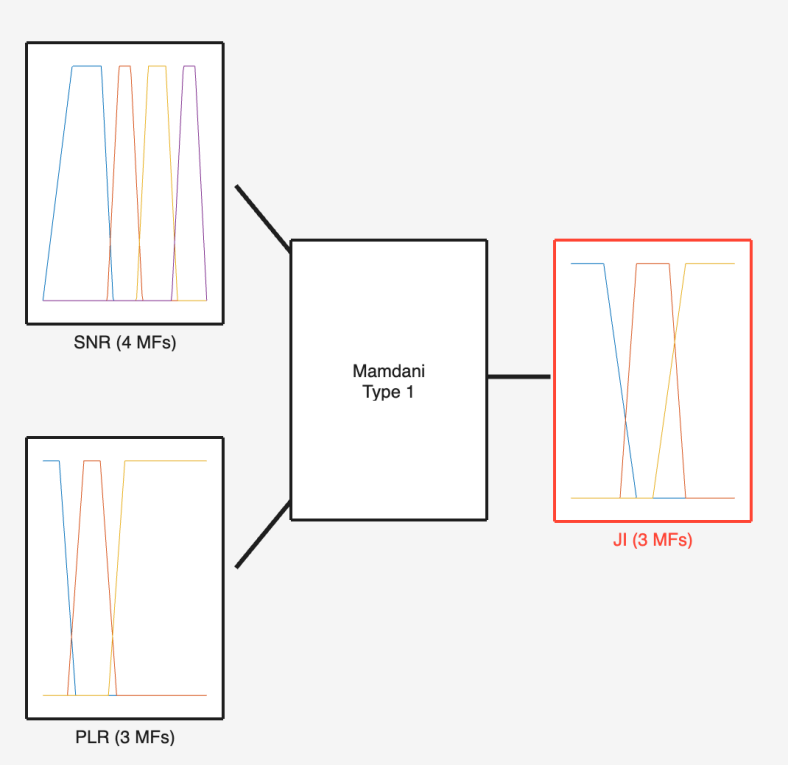


Figure 3.12: Structure of the Mamdani Fuzzy Inference System using SNR and PLR as inputs and Jamming Index (JI) as output

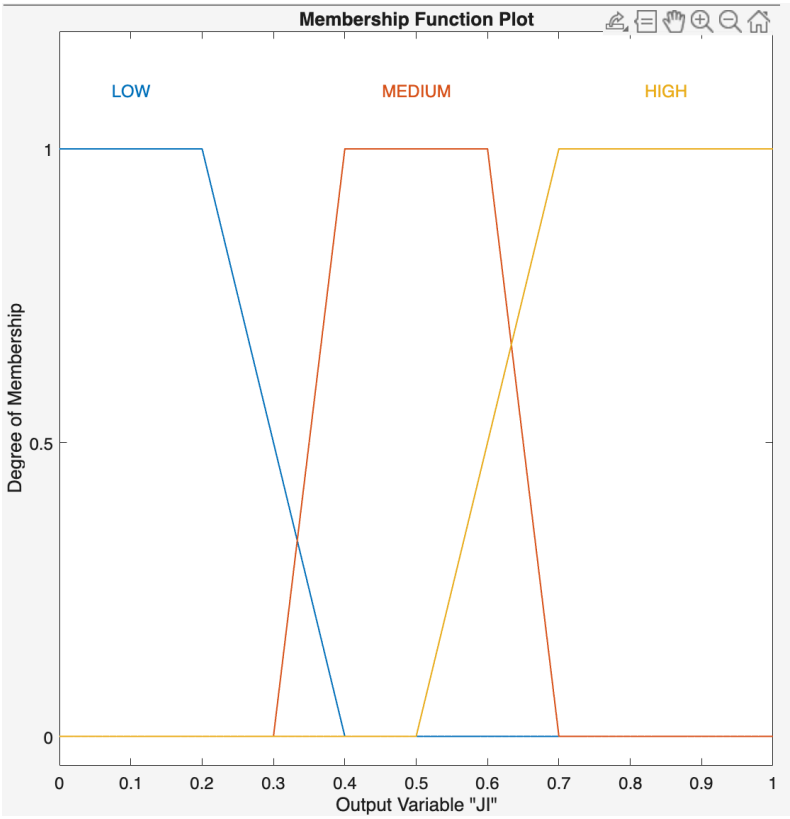


Figure 3.13: The Trapezoidal Membership Function Plot for Jamming Index (JI)

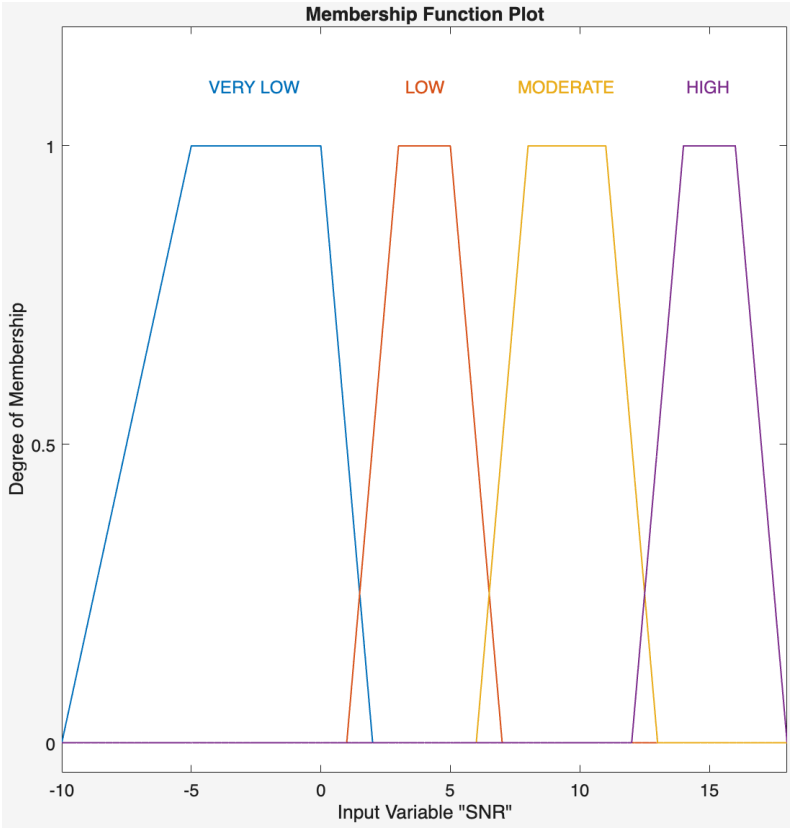


Figure 3.14: The Trapezoidal Membership Function Plot for SNR

Variable	Set	a	b	c	d
SNR (dB)	Very Low	-10	-5	0	2
	Low	1	3	5	7
	Moderate	6	8	11	13
	High	12	14	16	18
PLR	Low	0.0	0.0	0.1	0.2
	Moderate	0.15	0.25	0.35	0.45
	High	0.4	0.5	1.0	1.0
Jamming Index (JI)	Low	0.0	0.0	0.2	0.4
	Medium	0.3	0.4	0.6	0.7
	High	0.6	0.8	1.0	1.0

Table 3.5: Trapezoidal membership function parameters for SNR, PLR, and Jamming Index

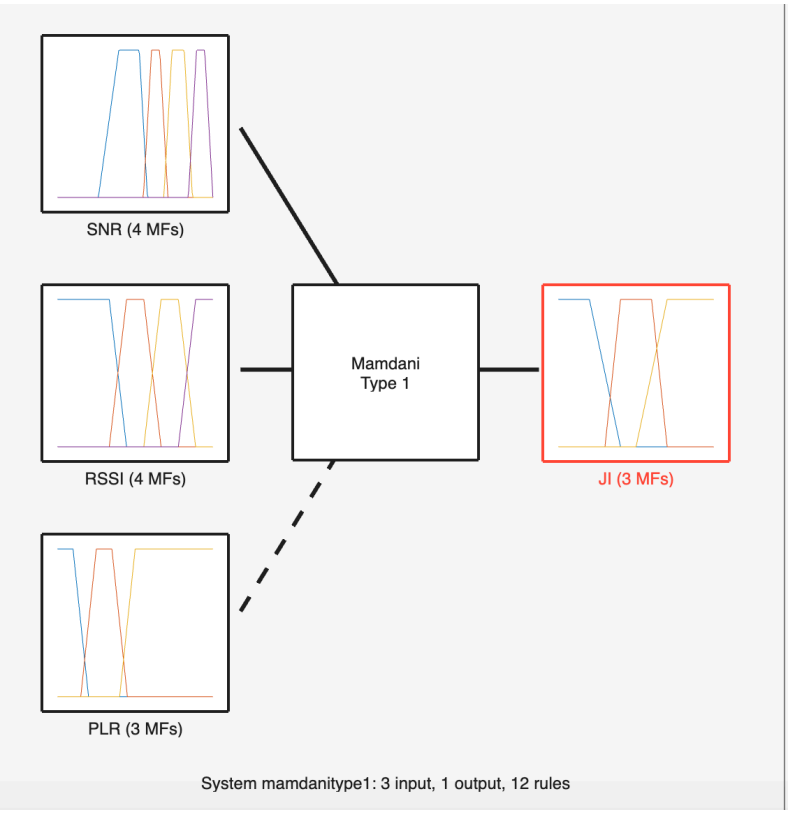


Figure 3.15: Structure of the Mamdani Fuzzy Inference System using RSSI, SNR, and PLR as inputs and Jamming Index (JI) as output

Variable	**Set**	**a**	**b**	**c**	**d**
RSSI (dBm)	Very Weak	-120	-120	-90	-80
	Weak	-90	-80	-70	-60
	Moderate	-70	-60	-50	-40
	Strong	-50	-40	-30	-30
SNR (dB)	Very Low	-10	-5	0	2
	Low	1	3	5	7
	Moderate	6	8	11	13
	High	12	14	16	18
PLR	Low	0.0	0.0	0.1	0.2
	Moderate	0.15	0.25	0.35	0.45
	High	0.4	0.5	1.0	1.0
Jamming Index (JI)	Low	0.0	0.0	0.2	0.4
	Medium	0.3	0.4	0.6	0.7
	High	0.5	0.7	1.0	1.0

Table 3.6: Trapezoidal membership function parameters for RSSI, SNR, PLR, and Jamming Index

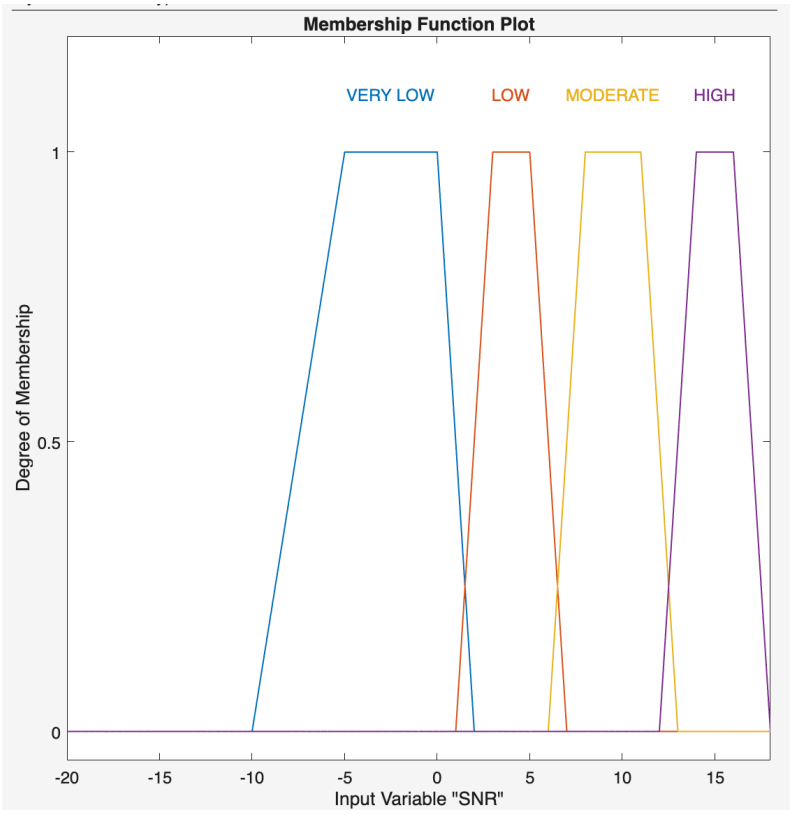


Figure 3.16: The Trapezoidal Membership Function Plot for SNR

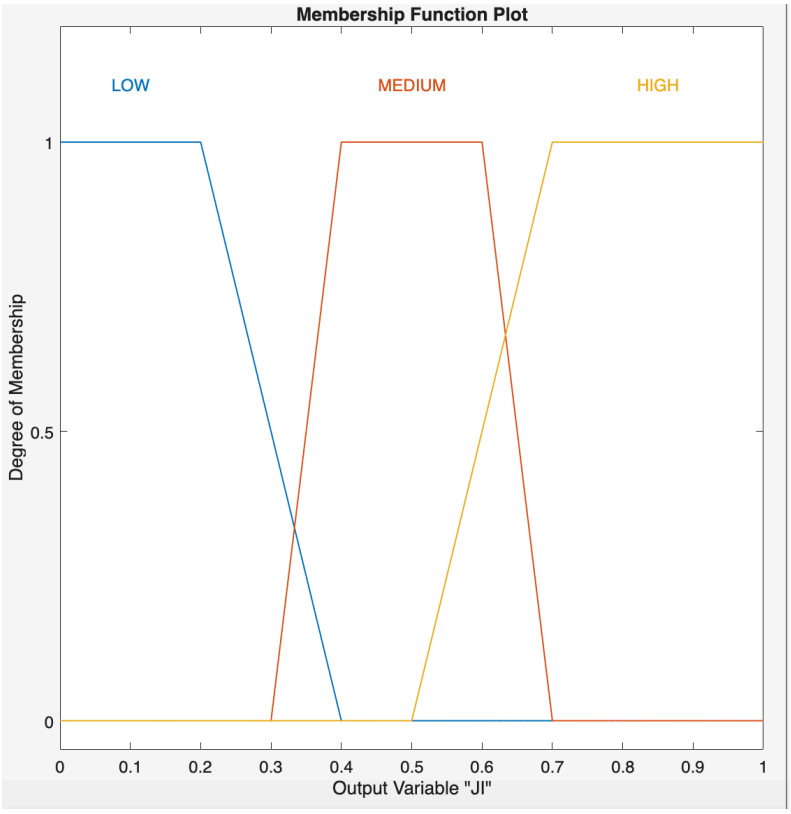


Figure 3.17: The Trapezoidal Membership Function Plot for Jamming Index (JI)

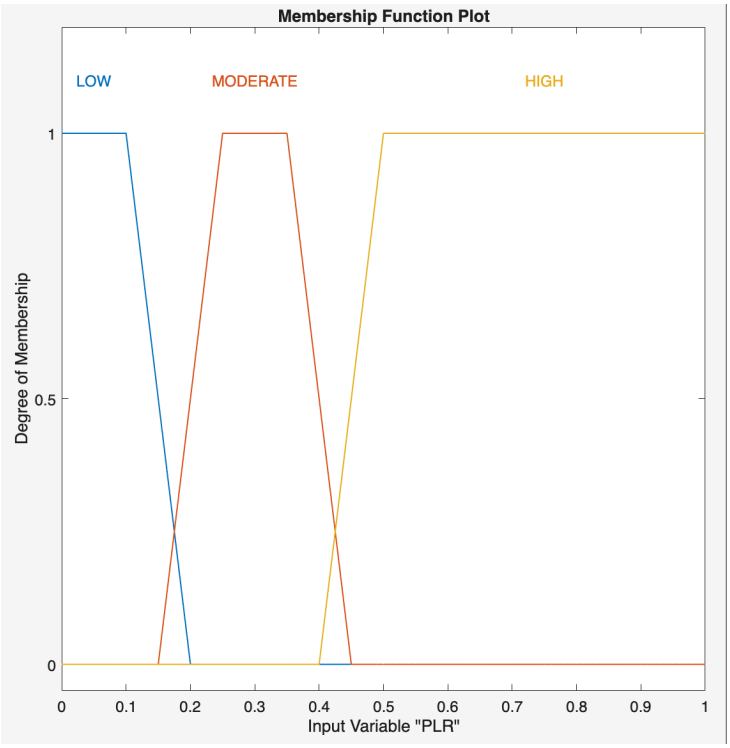


Figure 3.18: The Trapezoidal Membership Function Plot for PLR

4 Experimental Scenarios and Evaluation

This chapter presents a comprehensive evaluation of fuzzy rule-based jamming detection models using key signal metrics: Received Signal Strength Indicator (RSSI), Signal-to-Noise Ratio (SNR), and Packet Loss Rate (PLR). Given the severe class imbalance in the dataset (1.28% jamming vs. 98.72% normal traffic), standard accuracy metrics alone are insufficient. Instead, the analysis emphasizes precision, recall, and the F1 score to assess each model's ability to detect attacks reliably while minimizing false alarms. Multiple rule configurations are tested—ranging from aggressive detection strategies to highly conservative ones—to evaluate their trade-offs between sensitivity and specificity. The results highlight the strengths and limitations of each input feature combination, ultimately guiding the selection of an optimal detection strategy for real-world deployment.

4.1 Performance Evaluation Metrics

Several standard evaluation methods were employed to assess the efficiency of the jamming detection system. These metrics were selected with the dataset's significant class imbalance in mind (1.28% jamming vs. 98.72% normal instances), ensuring a statistically meaningful interpretation of performance.

Confusion Matrix: The classification results can first be summarized using a confusion matrix:

	Predicted	
	Jamming	**Normal**
Actual Jamming	TP	FN
Actual Normal	FP	TN

Table 4.1: Confusion Matrix for Jamming Attack Detection

A confusion matrix is a widely used performance evaluation tool in classification tasks. It visualizes and quantifies how effectively a model distinguishes between classes, displaying the outcomes in a 2×2 matrix that compares predicted and actual labels.

True Positive (TP): The model correctly predicts the positive class.
In our case: The model correctly identifies a jamming attack when one actually occurs.

False Positive (FP): The model incorrectly predicts the positive class.
In our case: The model mistakenly classifies normal network behavior as a jamming attack (false alarm).

True Negative (TN): The model correctly predicts the negative class.
In our case: The model correctly identifies normal network behavior as non-jamming.

False Negative (FN): The model fails to predict the positive class.
In our case: The model fails to detect an actual jamming attack, classifying it as normal activity—a serious security risk.

Accuracy quantifies the ratio of all correct predictions (both positive and negative) to the total number of instances. It is calculated as:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{4.1}$$

While accuracy is a useful initial indicator, it can be misleading in imbalanced datasets like ours (98.72% normal vs. 1.28% jamming). A model may achieve high accuracy simply by predicting the majority class, making this metric insufficient in isolation for security-critical applications. Therefore, additional metrics that reflect class distribution more effectively are required.

Precision evaluates the model's ability to correctly identify true jamming attacks while minimizing false alarms. It is defined as:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{4.2}$$

High precision indicates fewer false positives, which is crucial in operational security to avoid unnecessary disruptions. However, precision alone does not account for missed attacks, so it should be complemented with recall.

Recall quantifies the model's ability to detect actual jamming incidents:

$$\text{Recall} = \frac{TP}{TP + FN} \tag{4.3}$$

It calculates the proportion of true attacks correctly identified among all actual jamming events, including those missed by the model. In network security, minimizing undetected threats (false negatives) is paramount. Given that jamming events comprise only 1.28% of the dataset, recall is especially important for ensuring these rare but critical cases are detected. However, improving recall often increases false positives, potentially reducing precision.

F1 Score balances precision and recall by computing their harmonic mean:

$$\text{F1} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{4.4}$$

The F1 score is particularly suited to imbalanced classification tasks such as this. It combines

precision and recall into a single metric, offering a more balanced view of performance when neither false positives nor false negatives can be ignored. The score ranges from 0 to 1, with 1 indicating perfect detection and no false alarms. It is especially valuable for tuning decision thresholds where both types of errors have significant operational or security consequences.

These metrics allow us to quantify the system's performance in terms of:

- *Detection Sensitivity*: The ability to correctly identify actual jamming attacks.
- *Operational Precision*: The ability to minimize false alarms.

4.2 Evaluation of Fuzzy Rule Variants

To evaluate the effectiveness of fuzzy rule-based inference for jamming detection, a comprehensive analysis was performed for each combination of input features—RSSI, SNR, and PLR. For every input pair or triplet, multiple configurations of fuzzy rules were implemented, each defining how combinations of linguistic input values are mapped to linguistic outputs representing the likelihood of jamming. These rule variants were systematically tested and assessed using quantitative performance metrics: *accuracy, precision, recall, and F1 score*. Given the strong class imbalance in the dataset (only 1.28% of samples are labeled as jamming), particular emphasis was placed on recall and F1 score, as accuracy alone could be misleading.

4.2.1 Evaluation of Fuzzy Rule Variants for RSSI and SNR Combination

4.2.1.1 Rule Set A: Detection-Prioritized Mapping

This configuration emphasizes aggressive detection of potential jamming by assigning a high Jamming Index (JI) output to a broader range of moderate RSSI and SNR values. The rule logic is biased toward increasing the system's recall, thereby maximizing the detection of jamming instances—even at the cost of higher false positives. The complete fuzzy rule base is presented in Table 4.2.

RSSI	SNR	JI Output
Very Weak	Very Low	Low
Very Weak	Low	Medium
Very Weak	Moderate	Low
Very Weak	High	Medium
Weak	Very Low	Low
Weak	Low	Low
Weak	Moderate	Medium
Weak	High	High
Moderate	Very Low	Low
Moderate	Low	High
Moderate	Moderate	High
Moderate	High	High
Strong	Very Low	Low
Strong	Low	Medium
Strong	Moderate	High
Strong	High	High

Table 4.2: Fuzzy Rule Set A (RSSI and SNR)

Confusion Matrix:

	Predicted Jamming	Predicted Normal
Actual Jamming	241	167
Actual Normal	10,909	20,602

Table 4.3: Confusion Matrix for Rule Set A (RSSI and SNR)

Evaluation Metrics:

- **Accuracy:** 65.30%
- **Precision:** 2.16%
- **Recall:** 59.07%
- **F1 Score:** 4.17%

Rule Set A gives the best **recall** (59.07%) among all configurations tested, successfully identifying a majority of the actual jamming instances (241). However, this improvement in detection

comes at the expense of **precision** (2.16%), due to the significant number of false positives (10,909). This trade-off yields a very low F1 score of 4.17%, indicating that the rule set is particularly suitable for scenarios where detecting as many jamming events as possible is prioritized over minimizing false positives, such as in environments where the consequences of undetected attacks outweigh the cost of occasional false alarms.

The classification behavior under this rule set is further illustrated in the confusion matrix shown in Table 4.3, which visualizes the system's bias toward sensitivity by showing a high number of true positives alongside substantial false positives.

4.2.1.2 Rule Set B: Conservative Rule Set

In this rule set, the conditions that result in `High` JI outputs are limited to only a few strong input combinations. Most others are mapped to `Low` or `Medium`, resulting in a more conservative detection strategy that prioritizes minimizing false positives over maximizing jamming detection. The complete fuzzy rule base is presented in Table 4.4.

RSSI	**SNR**	**JI Output**
Very Weak	Very Low	Low
Very Weak	Low	Low
Very Weak	Moderate	Low
Very Weak	High	Medium
Weak	Very Low	Low
Weak	Low	Low
Weak	Moderate	Low
Weak	High	High
Moderate	Very Low	Low
Moderate	Low	Medium
Moderate	Moderate	High
Moderate	High	High
Strong	Very Low	Low
Strong	Low	Medium
Strong	Moderate	High
Strong	High	High

Table 4.4: Fuzzy Rule Set B (RSSI and SNR)

Evaluation Metrics:

- **Accuracy:** 93.20%
- **Precision:** 5.19%
- **Recall:** 25.00%
- **F1 Score:** 8.60%

Confusion Matrix:

Actual / Predicted	Jamming	Normal
Jamming	102	306
Normal	1863	29648

Table 4.5: Confusion Matrix for Rule Set B (RSSI and SNR)

Rule Set B yields high overall accuracy (93.20%) and significantly reduces the number of false positives compared to more aggressive rule sets. However, this comes at the cost of recall, capturing only 25% of actual jamming cases. The confusion matrix in Table 4.5 shows a large number of false negatives (306) compared to true positives (102), indicating under-detection. This configuration is appropriate in scenarios where reducing false alarms is more critical than maximizing detection coverage.

4.2.1.3 Rule Set C: Highly Restrictive Detection Strategy

This rule set represents a highly restrictive detection approach, where almost all input conditions are mapped to a `Low` Jamming Index (JI), with only a few exceptional cases escalating to `Medium` or `High`. The emphasis here is on avoiding false positives at nearly any cost, which results in extremely conservative classification behavior. The fuzzy rule mapping logic is detailed in Table 4.6.

RSSI	SNR	JI Output
Very Weak	Very Low	Low
Very Weak	Low	Low
Very Weak	Moderate	Low
Very Weak	High	Medium
Weak	Very Low	Low
Weak	Low	Low
Weak	Moderate	Low
Weak	High	Low
Moderate	Very Low	Low
Moderate	Low	Low
Moderate	Moderate	Low
Moderate	High	Medium
Strong	Very Low	Low
Strong	Low	Medium
Strong	Moderate	High
Strong	High	High

Table 4.6: Fuzzy Rule Set C (RSSI and SNR)

Evaluation Metrics:

- **Accuracy:** 98.72%
- **Precision:** 0.00%
- **Recall:** 0.00%
- **F1 Score:** 0.00%

Confusion Matrix:

Actual / Predicted	Jamming	Normal
Jamming	0	408
Normal	0	31511

Table 4.7: Confusion Matrix for Rule Set C (RSSI and SNR)

As shown in the confusion matrix (Table 4.7), this rule set completely fails to detect any of the 408 actual jamming cases, predicting every instance as `Normal`. While the overall accuracy is

high (98.72%), this is misleading due to the class imbalance in the dataset . The model effectively predicts the majority class only.

The recall and precision both are zero, indicating that the model does not generate any positive jamming predictions, and moreover cannot correctly identify even one attack. The F1 score is also zero, confirming that this rule set is functionally ineffective for jamming detection.

This setup may be suitable only in extreme edge cases where false positives are absolutely unacceptable — for example, in systems where false alarms trigger expensive or dangerous failsafes. However, for any scenario where actual threat detection is essential, this rule set is clearly inadequate.

4.2.1.4 Rule Set D: Aggressive Detection Mapping

This rule set is designed with an aggressive detection strategy that heavily prioritizes recall over precision. It assumes any moderate or low signal quality—particularly combinations of weak RSSI and low-to-moderate SNR to indicate potential jamming. As a result, a broad range of inputs are mapped to `High` Jamming Index (JI) values, maximizing the probability of detecting jamming events. The complete fuzzy rule base is presented in Table 4.8.

RSSI	**SNR**	**JI Output**
Very Weak	Very Low	Low
Very Weak	Low	High
Very Weak	Moderate	Medium
Very Weak	High	Medium
Weak	Very Low	Medium
Weak	Low	High
Weak	Moderate	High
Weak	High	High
Moderate	Very Low	Medium
Moderate	Low	High
Moderate	Moderate	High
Moderate	High	High
Strong	Very Low	Low
Strong	Low	Medium
Strong	Moderate	High
Strong	High	High

Table 4.8: Fuzzy Rule Set D (RSSI and SNR)

Confusion Matrix:

	Predicted Jamming	**Predicted Normal**
Actual Jamming	407	1
Actual Normal	31,505	6

Table 4.9: Confusion Matrix for Rule Set D(RSSI and SNR)

Evaluation Metrics:

- **Accuracy:** 1.29%
- **Precision:** 1.28%
- **Recall:** 99.75%
- **F1 Score:** 2.52%

Rule Set D achieves the highest recall across all evaluated rule sets, correctly detecting 407 out of 408 jamming events (99.75%). However, this comes at the severe cost of precision. Only 6 out of 31,511 normal samples were correctly classified, with the remaining majority misclassified as jamming. Consequently, the system raises nearly constant alarms, making it impractical for real-world deployment where false positives are costly or disruptive. This rule set may still hold value in safety-critical scenarios where failing to detect an attack is unacceptable, but it significantly compromises overall classification reliability and system usability.

As illustrated in the confusion matrix in Table 4.9, the model overwhelmingly predicts jamming regardless of the actual input, highlighting the need for a more balanced detection strategy in practical applications.

4.2.1.5 Results

Despite their theoretical complementarity, the RSSI and SNR combination did not perform well in detecting jamming activity in our dataset. One primary reason is that SNR values exhibited relatively small differences between normal and jamming conditions, as previously observed in the statistical analysis (mean SNR $\approx 10.89\,\text{dB}$ for jamming vs. $10.94\,\text{dB}$ for normal). This narrow margin limits the discriminative power of SNR in isolation.

Additionally, RSSI alone is not a reliable indicator of jamming, as it can be influenced by many benign environmental factors such as distance, or legitimate transmission power changes. When combined, both RSSI and SNR may fail to capture the reliability-related disruptions characteristic of jamming [26].

Moreover, the LoRaWAN environment used in the dataset exhibits considerable natural variability in both RSSI and SNR, even under normal conditions. This high baseline variance can mask the subtle shifts caused by jamming.

This performance gap motivated the decision to include Packet Loss Rate (PLR) as an input variable in subsequent models, as PLR more directly captures the impact of communication disruptions typical of jamming events.

4.2.2 Evaluation of Fuzzy Rule Variants for Combination PLR and RSSI

4.2.2.1 Rule Set A: Balanced Detection-Oriented Mapping

This rule set adopts a moderately aggressive detection strategy, where higher PLR values combined with increasingly stronger RSSI levels yield higher Jamming Index (JI) outputs. The goal is to capture a wide variety of jamming behaviors without being overly permissive. The complete rule table is shown in Table 4.10.

RSSI	PLR	JI Output
Very Weak	Low	Low
Very Weak	Moderate	Low
Very Weak	High	Medium
Weak	Low	Low
Weak	Moderate	Medium
Weak	High	High
Moderate	Low	Medium
Moderate	Moderate	High
Moderate	High	High
Strong	Low	Medium
Strong	Moderate	High
Strong	High	High

Table 4.10: Fuzzy Rule Set A (RSSI and PLR)

Evaluation Metrics:

- **Accuracy:** 61.53%
- **Precision:** 1.75%
- **Recall:** 52.70%
- **F1 Score:** 3.38%

Confusion Matrix:

Actual / Predicted	Jamming	Normal
Jamming	215	193
Normal	12085	19426

Table 4.11: Confusion Matrix for Rule Set A (RSSI and PLR)

This rule configuration demonstrates relatively high **recall** (52.70%)—capturing over half of the jamming events in the dataset. However, it also produces a substantial number of false positives (12,085), leading to a low precision (1.75%). The F1 score remains modest at 3.38%. This makes Rule Set A suitable for high-sensitivity applications where missing a jamming event is more detrimental than mistakenly raising an alarm.

4.2.2.2 Rule Set B: Over-Restrictive Detection Strategy

Rule Set B represents a highly conservative and restrictive mapping, where most input conditions are mapped to a `Low` Jamming Index (JI), even in cases of moderate or high PLR. Only a few specific combinations, mostly involving moderate RSSI and low PLR, escalate to higher JI levels. The rule design is outlined in Table 4.12.

RSSI	PLR	JI Output
Very Weak	Low	Low
Very Weak	Moderate	Low
Very Weak	High	Low
Weak	Low	High
Weak	Moderate	High
Weak	High	Low
Moderate	Low	High
Moderate	Moderate	High
Moderate	High	Low
Strong	Low	Medium
Strong	Moderate	High
Strong	High	High

Table 4.12: Fuzzy Rule Set (RSSI and PLR)

Evaluation Metrics:

- **Accuracy:** 98.72%
- **Precision:** 0.00%
- **Recall:** 0.00%
- **F1 Score:** 0.00%

Confusion Matrix:

Actual / Predicted	Jamming	Normal
Jamming	0	408
Normal	0	31,511

Table 4.13: Confusion Matrix for Rule Set B (RSSI and PLR)

This rule set performs well in terms of accuracy due to its tendency to classify all instances as `Normal`. However, this is a direct consequence of ignoring all jamming-related signal patterns. It achieves 0% recall, precision, and F1 score, meaning it fails to detect any jamming attacks. This result underscores that overly cautious mappings are inappropriate for scenarios requiring real-time threat response or anomaly detection.

4.2.2.3 Results

The combination of Packet Loss Rate (PLR) and Received Signal Strength Indicator (RSSI) produced substantially better results for jamming detection compared to models that relied on signal strength metrics alone. PLR, as a direct measure of transmission reliability, proved to be highly sensitive to communication disruptions typically caused by jamming events. In our dataset, PLR values showed a consistent upward shift during jamming episodes, offering a clear signal for detection.

The results that we got from this combination suggest that PLR is a crucial feature in capturing jamming effects, especially when combined with signal quality information from RSSI. While RSSI helps add spatial and physical-layer context, its variability under normal conditions makes it insufficient on its own. The fusion of PLR and RSSI therefore strikes a practical balance, where PLR brings reliability awareness and RSSI adds signal context, enabling fuzzy inference systems to more effectively model uncertain and imprecise behavior during jamming.

This combination demonstrated meaningful potential, especially under rule configurations that properly leverage PLR sensitivity.

4.2.3 Evaluation of Fuzzy Rule Variants for Combination PLR and SNR

4.2.3.1 Rule Set A: Detection-Biased Mapping

This rule set prioritizes detection by assigning higher Jamming Index (JI) values to a wide range of signal combinations. More precisely, to those that either SNR is very low or PLR is moderate or high. For example, all combinations involving `Very Low` or `Low` SNR and moderate-to-high PLR are mapped to `High`, indicating strong suspicion of jamming. Even when SNR is poor but PLR is low, the system still responds with a `Medium` JI output, suggesting that low-quality signals alone are a potential indicator of anomalous conditions.

As PLR increases, the rules elevate the suspicion level even further. Combinations of moderate SNR with high PLR also result in a `High` output, under the assumption that reliability degradation is a critical indicator of jamming even in the presence of acceptable signal clarity.

SNR	PLR	JI Output
Very Low	Low	Medium
Very Low	Moderate	High
Very Low	High	High
Low	Low	Medium
Low	Moderate	High
Low	High	High
Moderate	Low	Low
Moderate	Moderate	Medium
Moderate	High	High
High	Low	Low
High	Moderate	Low
High	High	Medium

Table 4.14: Fuzzy Rule Set A (SNR and PLR)

Evaluation Metrics:

- **Accuracy:** 61.53%
- **Precision:** 1.75%
- **Recall:** 52.70%
- **F1 Score:** 3.38%

Confusion Matrix:

Actual / Predicted	Jamming	Normal
Jamming	215	193
Normal	12085	19426

Table 4.15: Confusion Matrix for Rule Set A (SNR and PLR)

Rule Set A exhibits strong recall (52.70%), capturing more than half of the actual jamming cases. However, this comes with a significant number of false positives, leading to low precision (1.75%) and an F1 score of only 3.38%. This makes it more appropriate in cases where missing a jamming event is unacceptable, even if it means generating many false alarms.

4.2.3.2 Rule Set B: Precision-Focused Mapping

This rule set adopts a conservative strategy, producing `High` JI outputs only under very specific conditions—particularly where the PLR is low and SNR is poor. This set classifies combinations involving moderate or high PLR less aggressively, mapping them to `Low` even if signal quality (SNR) is degraded.

Notably, all combinations involving `High` PLR are mapped to `Low`, which severely restricts the system's ability to detect actual jamming, as PLR is a key indicator of transmission disruption. The logic focuses on catching cases where SNR is bad but reliability appears intact, which does not align well with typical jamming behavior.

SNR	PLR	JI Output
Very Low	Low	Medium
Very Low	Moderate	High
Very Low	High	High
Low	Low	Medium
Low	Moderate	High
Low	High	Low
Moderate	Low	High
Moderate	Moderate	Medium
Moderate	High	Low
High	Low	Low
High	Moderate	Low
High	High	Low

Table 4.16: Fuzzy Rule Set B (SNR and PLR)

Evaluation Metrics:

- **Accuracy:** 98.72%
- **Precision:** 66.67%
- **Recall:** 0.49%
- **F1 Score:** 0.97%

Confusion Matrix:

Actual / Predicted	Jamming	Normal
Jamming	2	406
Normal	1	31510

Table 4.17: Confusion Matrix for Rule Set B (SNR and PLR)

While Rule Set B achieves extremely high accuracy and precision (66.67%), this is misleading due to its almost complete failure to detect jamming events (recall = 0.49%). Only 2 out of 408 attacks were correctly flagged, making it unreliable in any scenario where jamming detection is a priority. It is best suited for scenarios where false alarms must be minimized, but at the severe cost of missing nearly all real attacks.

4.2.3.3 Results

The evaluation of fuzzy inference models using PLR and SNR as input features revealed a mixed performance profile, largely dependent on the chosen rule configuration.

The results illustrate that while PLR and SNR are useful indicators, their effectiveness is highly dependent on the rule logic applied. SNR on its own tends to be unreliable due to minimal statistical differences between jamming and normal conditions. PLR is a stronger feature due to its direct relationship with communication reliability, but its impact can be nullified if not properly emphasized in the rule design.

Overall, PLR and SNR together offer reasonable detection potential when the rules are biased toward recall (e.g., Rule Set A). However, without incorporating signal strength (RSSI) or temporal indicators, this combination may still be insufficient for robust and selective jamming detection. These findings suggest to integrate RSSI as a third input in subsequent models.

4.2.4 Evaluation of Fuzzy Rule Variants for Combination PLR, SNR and PLR

4.2.4.1 Rule Set A: Balanced Detection Strategy

This set of rules that is shown in Table 4.18 adopts a balanced strategy, where combinations of low SNR and high PLR (packet loss rate) are treated as strong evidence of jamming. However, a high RSSI can mitigate the final jamming indication (JI) score. The model prioritizes high JI predictions in cases of weak signal clarity and significant packet loss but remains conservative when RSSI is strong to minimize false alarms. This approach ensures reliable detection of jamming attacks while maintaining a low rate of erroneous alerts.

SNR	PLR	RSSI	JI Output
Very Low	Low	Very Weak	High
		Weak	High
		Moderate	High
		Strong	Medium
	Moderate	Very Weak	High
		Weak	High
		Moderate	High
		Strong	Medium
	High	Very Weak	High
		Weak	High
		Moderate	High
		Strong	High
Low	Low	Very Weak	High
		Weak	High
		Moderate	Medium
		Strong	Medium
	Moderate	Very Weak	High
		Weak	High
		Moderate	High
		Strong	Medium
	High	Very Weak	High
		Weak	High
		Moderate	High
		Strong	High
Moderate	Low	Very Weak	Medium
		Weak	High
		Moderate	Medium
		Strong	Low
	Moderate	Very Weak	High
		Weak	High
		Moderate	Medium
		Strong	Medium
	High	Very Weak	High
		Weak	High
		Moderate	Medium
		Strong	High
High	Low	Very Weak	Medium
		Weak	Low
		Moderate	Low
		Strong	Low
	Moderate	Very Weak	Medium
		Weak	Medium
		Moderate	Medium
		Strong	Low
	High	Very Weak	High
		Weak	High
		Moderate	Medium
		Strong	Medium

Table 4.18: Fuzzy Rule Set for SNR, PLR, and RSSI

Evaluation Metrics:

- **Accuracy:** 61.73%
- **Precision:** 1.74%
- **Recall:** 52.21%
- **F1 Score:** 3.37%

Confusion Matrix:

Actual / Predicted	Jamming	Normal
Jamming	213	195
Normal	12019	19492

Table 4.19: Confusion Matrix for Rule Set A (RSSI, SNR, PLR)

This configuration delivers robust recall (52.21%), highlighting its ability to detect a majority of jamming instances. However, the large number of false positives reduces precision, indicating that the model favors sensitivity over specificity. It's well-suited for security-critical deployments where missing an attack is more problematic than generating false alarms.

4.2.4.2 Rule Set B: Over-Restrictive Strategy

This rule set shown in Table 4.20 emphasizes conservativeness by suppressing the JI output in many borderline cases. Even when PLR is high, strong SNR or RSSI values lead to `Low` outputs, significantly reducing the system's alert frequency. Although it contains rules capable of high detection under very specific conditions, in practice it under-reports actual attacks.

SNR	PLR	RSSI	JI Output
Very Low	Low	Very Weak	High
		Weak	High
		Moderate	High
		Strong	Medium
	Moderate	Very Weak	High
		Weak	High
		Moderate	High
		Strong	Medium
	High	Very Weak	High
		Weak	Low
		Moderate	High
		Strong	High
Low	Low	Very Weak	High
		Weak	High
		Moderate	Medium
		Strong	Medium
	Moderate	Very Weak	High
		Weak	High
		Moderate	High
		Strong	Medium
	High	Very Weak	High
		Weak	Low
		Moderate	Low
		Strong	High
Moderate	Low	Very Weak	Medium
		Weak	High
		Moderate	Medium
		Strong	Low
	Moderate	Very Weak	High
		Weak	High
		Moderate	Medium
		Strong	Medium
	High	Very Weak	Low
		Weak	Low
		Moderate	Low
		Strong	High
High	Low	Very Weak	Medium
		Weak	Low
		Moderate	Low
		Strong	Low
	Moderate	Very Weak	Medium
		Weak	Low
		Moderate	Low
		Strong	Low
	High	Very Weak	High
		Weak	Low
		Moderate	Low
		Strong	Medium

Table 4.20: Compact Fuzzy Rule Set for SNR, PLR, and RSSI

Evaluation Metrics:

- **Accuracy:** 98.65%
- **Precision:** 0.00%
- **Recall:** 0.00%
- **F1 Score:** 0.00%

Confusion Matrix:

Actual / Predicted	Jamming	Normal
Jamming	0	408
Normal	24	31487

Table 4.21: Confusion Matrix for Rule Set B (RSSI, SNR, PLR)

Rule Set B nearly eliminates false positives but completely fails to detect any jamming events. It performs well in terms of accuracy only because of the extreme class imbalance, which makes such results misleading. The complete lack of recall and F1 score disqualifies this model for any application requiring reliable attack detection.

4.2.4.3 Rule Set C: Slightly More Aggressive Configuration

This set of rules in Table 4.22 introduces more aggressive mappings for moderate PLR and SNR conditions, especially when RSSI is weak or moderate. While still aiming to minimize unnecessary alerts, it includes more pathways to produce `High` JI, compared to the previous conservative version.

SNR	PLR	RSSI	JI Output
Very Low	Low	Very Weak	High
		Weak	High
		Moderate	High
		Strong	Medium
	Moderate	Very Weak	High
		Weak	High
		Moderate	High
		Strong	Medium
	High	Very Weak	High
		Weak	Low
		Moderate	High
		Strong	High
Low	Low	Very Weak	High
		Weak	High
		Moderate	Medium
		Strong	Medium
	Moderate	Very Weak	High
		Weak	High
		Moderate	High
		Strong	Medium
	High	Very Weak	High
		Weak	Low
		Moderate	High
		Strong	High
Moderate	Low	Very Weak	High
		Weak	High
		Moderate	High
		Strong	Low
	Moderate	Very Weak	High
		Weak	High
		Moderate	Medium
		Strong	Medium
	High	Very Weak	Low
		Weak	High
		Moderate	High
		Strong	High
High	Low	Very Weak	Medium
		Weak	Low
		Moderate	High
		Strong	Low
	Moderate	Very Weak	Medium
		Weak	Low
		Moderate	Low
		Strong	Low
	High	Very Weak	High
		Weak	Low
		Moderate	High
		Strong	Medium

Table 4.22: Fuzzy Rule Set for SNR, PLR, and RSSI

Evaluation Metrics:

- **Accuracy:** 66.61%
- **Precision:** 1.91%
- **Recall:** 49.75%
- **F1 Score:** 3.67%

Confusion Matrix:

Actual / Predicted	Jamming	Normal
Jamming	203	205
Normal	10452	21059

Table 4.23: Confusion Matrix for Rule Set C (RSSI, SNR, PLR)

Rule Set C finds a slightly better trade-off between recall and precision than Rule Set A, achieving the highest F1 score of the three. While not perfect, it is a strong candidate for applications that demand high detection coverage without overwhelming false alarms.

4.2.4.4 Results

The combination of RSSI, SNR, and PLR as input features produced better results than using signal strength metrics alone (RSSI and SNR). By integrating PLR—an indicator of communication reliability—into the fuzzy inference process, the model gained a more direct sensitivity to disruptions typically caused by jamming.

Among the tested rule sets, the highest recall achieved was approximately 52.21%, with an F1 score of 3.67%. It outperformed a lot of models based on RSSI and SNR alone, in most configurations. These improvements indicate that incorporating PLR provides valuable insight into the transmission layer, compensating for the weak discriminative power of SNR and the environmental variability of RSSI.

However, despite the added benefit of PLR, the combined model still suffered from a high false positive rate in most configurations. This is reflected in consistently low precision values (typically below 2%), which limited the F1 score improvements. Moreover, highly conservative rule sets that suppressed alerts in favor of high precision failed to detect jamming at all—highlighting the importance of balanced rule design.

In summary, this combination offers a more effective detection framework, especially when rule sets are tuned for moderate sensitivity. Nevertheless, the fuzzy model still faces limitations

in precision and would benefit from further refinement or additional features to enhance its practical deployment accuracy.

5 Conclusions and Future Work

This chapter summarizes the final findings of the study and outlines potential directions for future research. Focusing on LoRaWAN environments, the primary goal of this work was to investigate and evaluate the use of fuzzy logic-based models for detecting jamming attacks in Internet of Things (IoT) and Wireless Sensor Networks (WSNs). Specifically, the study assessed how well multiple physical- and link-layer metrics can contribute to the development of lightweight and interpretable intrusion detection systems based on fuzzy inference.

Summary of Results

A wide range of fuzzy rule configurations and membership function designs were tested across various combinations of the three selected input metrics. Performance was measured using accuracy, precision, recall, and F1 score—metrics that are especially important given the significant class imbalance in the dataset (only 1.28% of samples were labeled as jamming).

The main findings are summarized as follows:

- The combination of **RSSI and SNR** performed poorly in detecting jamming attacks. This was primarily due to the minimal variation in signal quality between normal and jamming conditions in the dataset. In many cases, similar RSSI and SNR values were observed in both benign and malicious transmissions, reducing their discriminative power when used in isolation.
- The use of **PLR and RSSI** or **PLR and SNR** produced better but mixed results. These combinations demonstrated that PLR is a more reliable indicator of jamming-related disruptions. While some rule sets achieved relatively high precision—indicating fewer false positives—they often failed to identify most jamming events. This reveals a trade-off between maximizing detection and minimizing false alarms. Furthermore, certain (SNR, PLR) or (RSSI, PLR) pairs appeared in both normal and jammed samples, which limited the system's ability to consistently distinguish between them.
- The best overall performance was achieved when using the **RSSI, SNR, and PLR** combination. This multi-dimensional input space enabled the fuzzy inference system to better capture a broader range of jamming behaviors, resulting in improved recall and F1 scores. The inclusion of PLR added a strong reliability measure, while RSSI and SNR provided additional physical-layer context to refine the detection process.

Limitations

The main limitation of this study lies in the characteristics of the dataset used. First, the dataset was highly imbalanced, with only approximately 1.28% of the entries labeled as jamming, which complicates model training and skews evaluation metrics such as accuracy. Second, the dataset included only a limited number of features that could be used—primarily RSSI, SNR, and PLR—restricting the ability to explore more complex or contextual indicators of jamming behavior. Additionally, the statistical analysis revealed that RSSI and SNR values showed considerable overlap between normal and jamming transmissions. Identical or near-identical signal values were frequently observed under both conditions, which reduced the discriminative power of these physical-layer features. These limitations constrained the effectiveness and generalizability of the fuzzy inference models.

Future Work

To enhance the robustness and adaptability of jamming detection systems, future research should consider the following directions:

Feature Preprocessing: Instead of relying solely on raw RSSI, SNR, and PLR values, future models could benefit from preprocessing these signals. Techniques such as computing moving averages, variances, or applying Exponentially Weighted Moving Averages (EWMA) over recent transmissions can smooth out transient fluctuations and highlight underlying patterns. For instance, EWMA has been effectively utilized to detect anomalies in network traffic by emphasizing recent changes while not entirely discarding older observations [49].

Trend Analysis: Beyond static measurements, analyzing the temporal trends of signal features can provide deeper insights into network behavior. Monitoring whether metrics like RSSI or PLR are consistently increasing, decreasing, or exhibiting periodic patterns can aid in distinguishing between normal variations and potential jamming activities. Time series analysis methods have been employed to detect such patterns, enhancing the detection of jamming attacks in wireless networks [50].

Feature Expansion: Future models should integrate a broader set of input features beyond RSSI, SNR, and PLR. This could include timing patterns (e.g., inter-packet arrival time), traffic behavior metrics, or contextual indicators such as device mobility or channel utilization, in order to improve detection robustness and reduce classification ambiguity.

Hybrid Approaches: Combining fuzzy logic with lightweight machine learning models (e.g., decision trees or rule-based learners) could yield hybrid detection systems that balance interpretability with adaptability, making them suitable for dynamic and resource-constrained IoT

environments.

Improved Dataset Collection: A more diverse and representative dataset is crucial for enhancing model training and evaluation. The current dataset suffers from strong class imbalance, limited feature diversity, and overlapping signal characteristics between normal and jamming conditions. A richer dataset that better captures the variety of jamming behaviors would significantly strengthen model generalizability and reliability.

Conclusion

This study reaffirms the potential of fuzzy inference systems as lightweight and interpretable solutions for jamming detection in IoT and wireless sensor networks. Fuzzy logic's capability to handle uncertainty and imprecise data makes it suitable for the nuanced nature of wireless communications.

However, the effectiveness of such systems is heavily influenced by the quality and diversity of input features. Sole reliance on raw physical-layer metrics like RSSI, SNR, and PLR may not capture the complex dynamics of jamming attacks. Incorporating preprocessing techniques and trend analyses can enhance the discriminative power of these features.

Furthermore, the development of comprehensive datasets that encompass a wide range of jamming scenarios and environmental conditions is essential. Such datasets will enable the training of more robust models capable of generalizing across different contexts.

In summary, while fuzzy inference systems hold promise for jamming detection, their success in real-world applications hinges on thoughtful feature engineering, hybrid modeling strategies, and the availability of rich, diverse datasets.

BIBLIOGRAPHY

[1] Monolithic Power Systems. (n.d.) Wireless sensing networks – advanced topics in sensing. Accessed: 2025-04-28. [Online]. Available: https://www.monolithicpower.com/en/learning/mpscholar/sensors/advanced-topics-in-sensing/wireless-sensing-networks

[2] R. Sadek, "Hybrid energy aware clustered protocol for iot heterogeneous network," *Future Computing and Informatics Journal*, vol. 3, 05 2018.

[3] Actility, "Lorawan architecture and network server," https://www.actility.com/lorawan-architecture-network-server/, 2025, accessed: 2025-05-15.

[4] T. Mitiku and M. Manshahia, "Neuro fuzzy inference approach : A survey," vol. 4, 04 2018.

[5] H. Soliman, A.-F. Attia, M. Hellal, and M. Badr, "Power system stabilizer driven by an adaptive fuzzy set for better dynamic performance," *Acta Polytechnica*, vol. 46, p. 3:10, 02 2006.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013, including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services Cloud Computing and Scientific Applications ‚Äî Big Data, Scalable Analytics, and Beyond. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X13000241

[7] S. R. Jino Ramson and D. J. Moni, "Applications of wireless sensor networks — a survey," in *2017 International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology (ICEEIMT)*, 2017, pp. 325–329.

[8] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[9] X. Yang, E. Karampatzakis, C. Doerr, and F. Kuipers, "Security vulnerabilities in lorawan," in *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2018, pp. 129–140.

[10] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, "Exploring the security vulnerabilities of lora," in *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*, 2017, pp. 1–6.

[11] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of lorawan," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 34–40, 2017.

[12] The Local SE, "Swedish planes grounded after air traffic control hit by gps jamming," 2015, available at: https://www.thelocal.se/20150409/swedish-air-traffic-hit-by-gps-jamming/ [Accessed: Apr. 21, 2025].

[13] A. Greenberg, "This $30 device stops a keyless car dead (and it's untraceable)," *WIRED*, 2015, https://www.wired.com/2015/08/hackers-can-steal-keyless-car/.

[14] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2005, pp. 46–57.

[15] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[16] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[17] S. Sharma, R. K. Bansal, and S. Bansal, "Issues and challenges in wireless sensor networks," in *2013 International Conference on Machine Intelligence and Research Advancement*, 2013, pp. 58–62.

[18] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[19] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 855–873, 2017.

[20] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: the rising stars in the iot and smart city scenarios," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 60–67, 2016.

[21] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128614003971

[22] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," 05 2005.

[23] RajaRatna and R. R. Ramaraj, "Survey on jamming wireless networks: Attacks and prevention strategies," 07 2022.

[24] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, “Jamming attacks on wireless networks: A taxonomic survey,” *International Journal of Production Economics*, vol. 172, pp. 76–94, 02 2016.

[25] F. T. Zahra, Y. S. Bostanci, and M. Soyturk, “Real-time jamming detection in wireless iot networks,” *IEEE Access*, vol. 11, pp. 70 425–70 442, 2023.

[26] N. Jeftenić, M. Simic, and Z. Stamenkovic, “Impact of environmental parameters on snr and rss in lorawan,” 06 2020.

[27] A. Lavric and V. Popa, “A lorawan: Long range wide area networks study,” in *2017 International Conference on Electromechanical and Power Systems (SIELMEN)*, 2017, pp. 417–420.

[28] M. Saban, M. Bekkour, I. Amdaouch, J. Gueri, B. Ait Ahmed, M. Z. Chaari, J. Ruiz-Alzola, A. Rosado, and O. Aghzout, “A smart agricultural system based on plc and a cloud computing web application using lora and lorawan,” *Sensors*, vol. 23, p. 2725, 03 2023.

[29] L. Zadeh, “Fuzzy logic,” *Computer*, vol. 21, no. 4, pp. 83–93, 1988.

[30] ——, “Soft computing and fuzzy logic,” *IEEE Software*, vol. 11, no. 6, pp. 48–56, 1994.

[31] M. Ramalingam and A. Baskaran, “A comprehensive study on fuzzy inference system and its application in the field of engineering,” 12 2017.

[32] J. Dickerson and J. Dickerson, “Fuzzy network profiling for intrusion detection,” in *Peach-Fuzz 2000. 19th International Conference of the North American Fuzzy Information Processing Society - NAFIPS (Cat. No.00TH8500)*, 2000, pp. 301–306.

[33] E. Mamdani and S. Assilian, “An experiment in linguistic synthesis with a fuzzy logic controller,” *International Journal of Man-Machine Studies*, vol. 7, no. 1, pp. 1–13, 1975. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0020737375800022

[34] H.-J. Zimmermann, *Fuzzy Set Theory – and Its Applications*, 01 2001, vol. 2001.

[35] H. Reyes Moncayo and N. Kaabouch, “Jamming and lost link detection in wireless networks with fuzzy logic,” *International Journal of Scientific and Engineering Research*, vol. 4, 02 2013.

[36] M. Savva, I. Ioannou, and V. Vassiliou, “Fuzzy-logic based ids for detecting jamming attacks in wireless mesh iot networks,” in *2022 20th Mediterranean Communication and Computer Networking Conference (MedComNet)*, 2022, pp. 54–63.

[37] M. M. Patel and A. Aggarwal, “Security attacks in wireless sensor networks: A survey,” in *2013 International Conference on Intelligent Systems and Signal Processing (ISSP)*, 2013, pp. 329–333.

[38] J. Deogirikar and A. Vidhate, “Security attacks in iot: A survey,” in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017, pp. 32–37.

[39] S. M. Danish, A. Nasir, H. K. Qureshi, A. B. Ashfaq, S. Mumtaz, and J. Rodriguez, “Network intrusion detection system for jamming attack in lorawan join procedure,” in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1–6.

[40] M. A. Haque and A. Saifullah, “Handling jamming attacks in a lora network,” in *2024 IEEE/ACM Ninth International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2024, pp. 146–157.

[41] G. Morillo, U. Roedig, and D. Pesch, “Detecting targeted interference in nb-iot,” in *2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)*, 2023, pp. 475–482.

[42] M. Savva, “A framework for the detection, localization, and recovery from jamming attacks in the internet of things,” Doctoral Thesis, University of Cyprus, Nicosia, Cyprus, 2024.

[43] A. Proto, C. C. Miers, and T. C. M. B. Carvalho, “Classification and characterization of lorawan energy depletion attacks: A review,” *IEEE Sensors Journal*, vol. 25, no. 2, pp. 2141–2156, 2025.

[44] M. Abdollahi, K. Malekinasab, W. Tu, and M. Bag-Mohammadi, “An efficient metric for physical-layer jammer detection in internet of things networks,” in *2021 IEEE 46th Conference on Local Computer Networks (LCN)*, 2021, pp. 209–216.

[45] B. B. Zarpel√£o, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, “A survey of intrusion detection in internet of things,” *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804517300802

[46] N. S. Senol, A. Rasheed, M. Baza, and M. Alsabaan, “Identifying tampered radio-frequency transmissions in lora networks using machine learning,” *Sensors*, vol. 24, no. 20, 2024. [Online]. Available: https://www.mdpi.com/1424-8220/24/20/6611

[47] P. Bhattacharjee, A. Shahin, and F. Begum, “Fuzzy approach for intrusion detection system: A survey,” *International Journal of Computer Applications*, vol. 61, no. 20, pp. 1–5, 02 2013.

[48] D. R. Bhadra, C. A. Joshi, P. R. Soni, N. P. Vyas, and R. H. Jhaveri, “Packet loss probability in wireless networks: A survey,” in *2015 International Conference on Communications and Signal Processing (ICCSP)*, 2015, pp. 1348–1354.

[49] O. Osanaiye, A. Alfa, and G. Hancke, “A statistical approach to detect jamming attacks in wireless sensor networks,” *Sensors*, vol. 18, 05 2018.

[50] M. Cheng, Y. Ling, and W. Wu, “Time series analysis for jamming attack detection in wireless networks,” 12 2017, pp. 1–7.