

Original Research

Received 03 June 2026

Revised 18 July 2026

Accepted 01 Aug 2026

Natural Resources for Human Health 2026, Vol. 6 (15s): 130–164

KEYWORDS:

Internet of Things (IoT), Selective Jamming Attacks, Packet Hiding Techniques, Adaptive Packet Transmission, Machine Learning–Based Attack Detection, Wireless Network Security, Anti-Jamming Mechanisms, Secure IoT Communication, Adversarial Resilience

A Novel Packet Hiding Approach for Preventing Jamming Attacks in Internet of Things Environment

Ms. Priya Bhatt¹, Dr. Rakesh Kumar², Dr. Vandana Sharma³

¹Research Scholar, Department of Computer Science & Engineering Rabindranath Tagore University, Pune-411048, Maharashtra, India.

²Research Guide, Department of Computer Science & Engineering Rabindranath Tagore University, SPune-411048, Maharashtra, India.

³Associate professor, Department of Computer Science and Engineering, Christ University Delhi NCR, India. vandana.juyal@gmail.com

Corresponding Author email: priyabhatt58@gmail.com, rakesh.kumar@aisectunivetsity.ac.in

ABSTRACT: The rapid proliferation of Internet of Things (IoT) devices has significantly increased the reliance on wireless communication, thereby exposing IoT networks to a wide range of security threats, particularly selective and intelligent jamming attacks. Such attacks exploit vulnerabilities in existing IoT communication protocols by targeting critical packets, leading to severe degradation in network performance, reliability, and availability. This research aims to analyze the inherent weaknesses of current IoT communication mechanisms and proposes a novel packet hiding approach to mitigate jamming attacks effectively. The proposed methodology integrates adaptive packet transmission strategies with machine learning–based detection mechanisms to obscure packet characteristics such as timing, size, and transmission patterns, making them indistinguishable to adversarial jammers. The system dynamically adjusts transmission parameters based on real-time network conditions and detected threat levels, thereby enhancing resilience against both static and adaptive jamming attacks. Performance evaluation is conducted using simulation-based experiments, comparing the proposed approach with existing anti-jamming techniques in terms of packet delivery ratio, throughput, latency, energy efficiency, and attack detection accuracy. The expected outcomes demonstrate significant improvements in secure packet transmission, robustness against adversarial interference, and overall network reliability. In conclusion, this work provides a comprehensive and practical security framework for IoT environments, contributing to both academic research and real-world deployment by strengthening the resilience of critical wireless communication systems against jamming attacks.

1. INTRODUCTION

1.1 Background and Motivation

The Internet of Things (IoT) has emerged as a transformative paradigm that interconnects billions of heterogeneous devices, enabling intelligent data sensing, processing, and communication across diverse application domains such as smart healthcare, industrial automation, environmental monitoring, and smart cities. These systems predominantly rely on wireless communication technologies due to their flexibility, scalability, and cost efficiency. However, the open and broadcast nature of wireless channels exposes IoT networks to severe security threats that can compromise availability, reliability, and quality of service. Among these threats, jamming attacks are particularly destructive as they directly target the physical and medium access

control layers, rendering traditional cryptographic security mechanisms ineffective. Unlike conventional cyberattacks that focus on data confidentiality or integrity, jamming attacks disrupt communication by injecting malicious radio interference, leading to packet loss, increased latency, and network outages. Studies have shown that even low-power jammers can significantly degrade network performance by selectively targeting critical packets [Xu et al., 2005], [Gollakota et al., 2011]. The motivation behind this research lies in addressing the inadequacy of existing anti-jamming solutions for resource-constrained IoT environments and developing a proactive, lightweight, and intelligent packet hiding mechanism capable of preventing selective jamming attacks while preserving energy efficiency and communication reliability.

1.2 Internet of Things (IoT) Architecture and Communication Models

IoT systems are typically organized into a layered architecture consisting of the perception layer, network layer, and application layer, each serving a distinct functional role. The perception layer comprises sensors, actuators, and embedded devices responsible for collecting real-time data from the physical environment. The network layer facilitates data transmission using wireless technologies such as IEEE 802.15.4, ZigBee, LoRaWAN, NB-IoT, and Wi-Fi, often operating under strict energy and bandwidth constraints. The application layer provides data analytics, visualization, and decision-making services tailored to specific use cases. Communication models in IoT include device-to-device, device-to-gateway, and device-to-cloud interactions, which introduce varying latency, scalability, and security requirements. Due to the lightweight nature of IoT protocols, packet structures and transmission patterns are often predictable, making them vulnerable to traffic analysis and selective interference attacks. Furthermore, centralized communication models increase the risk of single points of failure under jamming conditions [Atzori et al., 2010], [Al-Fuqaha et al., 2015]. These architectural and communication characteristics necessitate robust anti-jamming mechanisms that can operate across layers while maintaining compatibility with constrained IoT devices.



Figure 1.1: Packet Hiding Approach for IoT Security

1.3 Security Challenges in IoT Networks

Security in IoT networks is a multifaceted challenge arising from device heterogeneity, limited computational resources, dynamic topologies, and large-scale deployments. IoT devices often lack sufficient processing power and memory to support complex security protocols, making them susceptible to attacks such as spoofing, replay attacks, denial-of-service, and jamming. Additionally, IoT networks are frequently deployed in unattended or hostile environments, increasing the likelihood of physical and insider attacks. Jamming attacks are especially problematic because they do not require compromising cryptographic keys or authentication mechanisms; instead, attackers exploit physical-layer vulnerabilities to disrupt communication. [Roman et al., 2013], [Sicari et al., 2015]. The inability of conventional security techniques to guarantee availability under jamming conditions poses a serious threat to mission-critical applications. Prior research highlights that ensuring reliable communication in the

presence of intelligent adversaries remains an open research challenge, particularly for low-power IoT systems. Consequently, new security solutions must focus not only on detection but also on prevention and resilience against adaptive attacks.

1.4 Jamming Attacks in Wireless IoT Environments

Jamming attacks in wireless IoT environments aim to intentionally interfere with legitimate signal transmissions by emitting malicious radio signals within the same frequency band. These attacks can drastically reduce network throughput, increase packet loss, and disrupt time-critical communications. Due to the low transmission power and static communication schedules of IoT devices, attackers can efficiently identify and exploit vulnerable transmission windows. Unlike random interference, jamming attacks are often carefully crafted to maximize damage while minimizing attacker energy consumption. Research indicates that jamming attacks can lead to cascading failures in multi-hop IoT networks by disrupting routing and control messages [Xu et al., 2006]. As IoT applications increasingly support safety-critical operations, the impact of such attacks becomes even more severe, underscoring the need for robust, adaptive, and intelligent anti-jamming solutions.

Types of Jamming Attacks Jamming attacks are generally categorized into constant, deceptive, random, and reactive jamming. Constant jammers continuously transmit high-power noise signals, causing persistent interference but consuming significant energy. Deceptive jammers inject fabricated packets to confuse legitimate nodes and disrupt protocol operations. Random jammers alternate between active and inactive states to conserve energy and evade detection. Reactive jammers remain silent until they detect legitimate transmissions and then immediately interfere, making them difficult to identify using conventional detection techniques. Among these, reactive jamming poses the greatest threat to IoT networks due to its efficiency and stealthy behavior [Wood et al., 2007], [Law et al., 2018].

Selective and Intelligent Jamming Selective and intelligent jamming represents an advanced form of reactive jamming where attackers exploit protocol knowledge to selectively target high-value packets such as routing updates, acknowledgments, or synchronization messages. By performing real-time packet classification, intelligent jammers can disrupt network functionality with minimal transmissions. Studies demonstrate that selective jammers can achieve the same level of disruption as constant jammers while using significantly less energy [Gollakota et al., 2011]. These attacks are particularly effective against IoT networks due to predictable packet formats and periodic transmission patterns. Preventing selective jamming requires mechanisms that conceal packet semantics and timing information, thereby preventing adversaries from distinguishing critical packets [Pelechrinis et al., 2011].

1.5 Limitations of Existing Anti-Jamming Techniques

Existing anti-jamming techniques such as frequency hopping, spread spectrum, power control, and channel diversity have been widely studied in traditional wireless networks. However, their applicability to IoT environments is limited due to high energy consumption, synchronization overhead, and computational complexity. Many existing solutions focus on detecting jamming after it has already caused disruption, rather than preventing it proactively. Moreover, these techniques often assume static or non-adaptive attackers, making them ineffective against intelligent jammers capable of learning network behavior. Packet hiding approaches proposed in earlier studies demonstrate promise but lack adaptability and scalability for dynamic IoT scenarios [Xu et al., 2005], [Sekhar et al., 2013]. These limitations highlight the need for a novel packet hiding approach combined with adaptive transmission strategies to proactively defend against selective jamming attacks while maintaining efficiency and practicality in IoT networks.

2 OVERVIEW OF IOT SECURITY MECHANISMS

The Internet of Things (IoT) paradigm introduces a large-scale interconnected ecosystem composed of heterogeneous, resource-constrained devices that operate in dynamic and often hostile environments. Ensuring security in such systems is challenging due to the limited computational capabilities, energy constraints, and scalability requirements of IoT devices. Existing IoT security mechanisms primarily focus on conventional security objectives such as confidentiality, integrity, authentication, and access control. Lightweight cryptographic algorithms, key management schemes, and secure communication protocols have been proposed to address these constraints [Roman et al., 2013]. In addition, intrusion detection systems and trust-based frameworks have been explored to identify malicious behavior within IoT networks [Sicari et al., 2015]. However, most of these approaches operate at the network or application layer and do not sufficiently address physical-layer threats.

Jamming attacks, which directly disrupt wireless communication by injecting malicious interference, remain largely unmitigated by traditional security mechanisms. This limitation motivates the exploration of proactive and cross-layer security solutions that can ensure availability and resilience against jamming attacks in IoT environments.

2.1 Existing Jamming Detection and Mitigation Techniques

Numerous techniques have been proposed in the literature to detect and mitigate jamming attacks in wireless networks. Early detection methods relied on monitoring signal strength indicators, packet delivery ratio, and carrier sensing time to identify abnormal interference patterns [Xu et al., 2006]. Mitigation approaches such as frequency hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS), and channel surfing have been shown to be effective in traditional wireless networks. However, these techniques impose significant energy, synchronization, and hardware overhead, rendering them impractical for resource-constrained IoT devices. Recent studies have explored adaptive and intelligent approaches using game theory and reinforcement learning to counter reactive and adaptive jammers [Alsulami et al., 2021]. Although these methods improve resilience, they often require continuous learning and extensive training data, which limits their applicability in real-time IoT deployments. Furthermore, most existing techniques focus on reacting to jamming rather than preventing it proactively, leaving IoT networks vulnerable to selective and intelligent jamming attacks.

2.2 Packet Hiding and Obfuscation Approaches

Packet hiding and obfuscation have emerged as promising strategies for preventing selective jamming attacks by concealing packet characteristics from adversaries. These approaches aim to hide critical packet information such as headers, packet size, timing, or transmission patterns, thereby preventing attackers from distinguishing high-value packets. [Gollakota et al.] introduced cryptographic packet hiding techniques that encrypt packet headers to thwart selective jamming [Gollakota et al., 2011]. Other studies have explored packet padding, random delays, and traffic shaping to obfuscate communication patterns [Pelechrinis et al., 2011]. While these methods demonstrate effectiveness against selective jamming, they often introduce additional latency and energy overhead. Moreover, static obfuscation strategies fail to adapt to intelligent adversaries capable of learning network behavior. Consequently, recent research emphasizes the need for adaptive packet hiding mechanisms that dynamically adjust obfuscation parameters based on network conditions and threat levels, particularly in IoT environments.

2.3 Machine Learning Techniques for Attack Detection

Machine learning (ML) techniques have gained significant attention for enhancing security in wireless and IoT networks due to their ability to learn complex patterns and adapt to evolving threats. ML-based approaches enable automated detection of anomalous behavior by analyzing traffic features such as packet rate, signal strength, and delay variations. These methods offer advantages over rule-based systems by improving detection accuracy and reducing false positives [Chen et al., 2021]. In the context of jamming attacks, ML models can distinguish between normal interference and malicious jamming, even in dynamic environments. However, the effectiveness of ML techniques depends on the availability of representative data and the computational feasibility of deploying models on constrained devices.

Supervised Learning Methods

Supervised learning techniques such as Support Vector Machines (SVM), Random Forests, and Neural Networks have been widely used for jamming and intrusion detection. These models are trained using labeled datasets to classify network states as normal or under attack. Studies report high detection accuracy when sufficient labeled data is available [Li et al., 2020]. However, supervised methods suffer from scalability issues and poor generalization to unseen attack patterns. Additionally, the requirement for labeled training data limits their applicability in real-world IoT scenarios, where attack behaviors continuously evolve.

Unsupervised and Adaptive Learning Methods:

Unsupervised and adaptive learning methods, including clustering algorithms and reinforcement learning, address the limitations of supervised techniques by learning patterns without labeled data. These approaches are particularly suitable for detecting novel and adaptive jamming attacks. Reinforcement learning-based anti-jamming strategies enable IoT nodes to dynamically adjust transmission parameters such as frequency and power based on environmental feedback [Chen et al., 2021].

Despite their adaptability, these methods often involve long convergence times and computational complexity, which can be challenging for real-time IoT applications.

2.4 Comparative Analysis of Existing Techniques

A comparative analysis of existing anti-jamming techniques reveals significant trade-offs between effectiveness, energy efficiency, adaptability, and deployment complexity. Traditional physical-layer techniques provide robustness but are resource-intensive, while packet hiding approaches offer proactive defense but may introduce latency. Machine learning-based solutions improve detection accuracy but require careful model design to suit IoT constraints. The literature indicates a clear research gap in integrating lightweight packet hiding mechanisms with adaptive machine learning-based transmission strategies to proactively prevent selective jamming attacks while maintaining efficiency and scalability. Addressing this gap forms the foundation of the proposed research.

3. SYNTHESIS OF PREVIOUS RESEARCH

The synthesis of previous research consolidates major findings from studies on IoT security, wireless communication vulnerabilities, jamming attacks, packet hiding mechanisms, and machine learning-based defense strategies. Existing literature consistently indicates that while IoT networks enable scalable and energy-efficient communication, their dependence on wireless channels and lightweight protocols exposes them to severe physical-layer threats, particularly selective and intelligent jamming attacks [3-18][41-76]. Most security mechanisms proposed for IoT environments primarily focus on confidentiality, integrity, and authentication, offering limited protection against attacks that target network availability and communication reliability [7-29][63-95]. Research on jamming attacks demonstrates that traditional mitigation techniques such as frequency hopping, spread spectrum, and channel hopping are effective in conventional wireless networks but introduce significant energy consumption, synchronization complexity, and hardware overhead when applied to IoT systems [12-34] [58-82]. Furthermore, many of these approaches are reactive in nature and fail to prevent intelligent jammers that adapt their attack strategies based on real-time network observations [21-49-71]. Studies on selective jamming reveal that adversaries can exploit predictable packet formats, timing patterns, and protocol-specific characteristics to disrupt critical transmissions with minimal energy expenditure [16-37] [66-104].

Packet hiding and obfuscation techniques have been widely explored as proactive countermeasures to selective jamming attacks. Prior research highlights that concealing packet headers, normalizing packet sizes, and randomizing transmission timing can significantly reduce the effectiveness of intelligent jammers [11-28] [53-90]. However, many existing packet hiding approaches employ static obfuscation parameters and introduce additional latency and computational overhead, limiting their adaptability and efficiency in dynamic IoT environments [24-45] [69-97]. These limitations reduce their resilience against adversaries capable of learning and adapting to network behavior. Machine learning-based approaches have gained attention for enhancing jamming detection and mitigation by enabling adaptive and data-driven decision-making. Supervised and unsupervised learning models have demonstrated improved detection accuracy and robustness against evolving attack patterns [5-32-57-83]. Nevertheless, the literature also points out challenges related to model complexity, training data availability, and real-time deployment on resource-constrained IoT devices [14-48-73-108]. The computational overhead associated with advanced learning models often limits their practical applicability in large-scale IoT networks.

3.1 Threat Model and Assumptions

The threat model considered in this work assumes the presence of a powerful and intelligent jammer capable of performing selective jamming attacks. The adversary is assumed to continuously monitor the wireless channel and perform real-time packet inspection to identify high-value packets such as control messages, routing updates, or acknowledgment frames. Based on this analysis, the jammer selectively injects interference to disrupt only critical communications, thereby maximizing network disruption while minimizing energy consumption.

It is assumed that the attacker has knowledge of IoT protocols, packet formats, and transmission schedules but does not possess cryptographic keys or access to internal system parameters. The jammer operates in a reactive and adaptive manner, enabling it to evade simple detection mechanisms. The IoT nodes are assumed to be resource-constrained and deployed in an open wireless

environment. Physical compromise of nodes and insider attacks are beyond the scope of this study. These assumptions are consistent with widely accepted selective jamming threat models in existing literature [7][31][54][102].

3.2 Proposed Novel Packet Hiding Approach

The proposed packet hiding approach serves as the core defense mechanism against selective jamming attacks. The fundamental idea is to prevent adversaries from distinguishing between different types of packets by concealing observable packet characteristics at the physical and MAC layers. Instead of relying solely on encryption, which protects payload content but leaves metadata exposed, the proposed method focuses on obfuscating packet headers, transmission timing, and packet size patterns. By ensuring statistical similarity among all transmitted packets, the jammer is deprived of the information required for packet classification and selective interference. This proactive defense significantly reduces the effectiveness of intelligent jamming attacks while maintaining efficient communication. The packet hiding mechanism is lightweight and adaptable, making it suitable for deployment in large-scale IoT networks [12][28][63][91].

3.3 Packet Feature Obfuscation Mechanism

Packet feature obfuscation aims to conceal protocol-specific identifiers and control information that can be exploited by intelligent jammers for packet classification. In the proposed system, critical header fields such as packet type, sequence identifiers, and control flags are masked using lightweight cryptographic operations. Additionally, dummy header fields and controlled randomness are introduced to prevent attackers from inferring packet semantics through statistical analysis. This mechanism ensures that all packets appear indistinguishable at the physical layer, thereby preventing selective targeting of high-value transmissions. The obfuscation process is carefully designed to minimize computational overhead and avoid excessive energy consumption. By combining encryption with structural obfuscation, the proposed mechanism enhances robustness against both known and unknown jamming strategies [16][42][70][95].

Timing and Size Randomization Strategy Intelligent jammers often exploit predictable packet timing and size patterns to infer packet importance. To counter such traffic analysis attacks, the proposed system introduces controlled randomization in packet transmission timing and packet size. Random delays are added to packet transmission within predefined bounds to obscure temporal correlations between network events and packet transmissions. Packet padding techniques are employed to normalize packet sizes, ensuring uniformity across different packet types. These randomization strategies are dynamically adjusted based on network conditions to balance security and performance. By disrupting timing- and size-based inference, the proposed strategy significantly reduces the jammer's ability to perform selective interference while maintaining acceptable latency and throughput levels [22][49][77][104].

3.4 Adaptive Packet Transmission Strategy

To further enhance resilience against jamming attacks, the proposed system incorporates an adaptive packet transmission strategy that dynamically adjusts communication parameters based on environmental feedback. This strategy enables IoT nodes to respond intelligently to varying channel conditions and detected threat levels. Instead of using static transmission parameters, the system continuously monitors network performance metrics and adapts transmission behavior to minimize jamming impact. This adaptive approach improves reliability and ensures efficient spectrum utilization under adversarial conditions [6][33][61].

Dynamic Transmission Control Dynamic transmission control enables IoT nodes to modify transmission parameters such as transmission power, packet rate, and retransmission policies in response to detected interference. When jamming activity is suspected, the system reduces transmission predictability by altering packet schedules and transmission intensity. This adaptability makes it difficult for jammers to anticipate transmission behavior and execute effective attacks. The control mechanism operates with minimal overhead and is designed to converge quickly, ensuring timely response to jamming threats without disrupting normal communication [14][40][68][96].

Channel Condition Awareness Channel condition awareness plays a critical role in adaptive transmission by enabling nodes to assess the quality of the wireless channel in real time. Metrics such as signal-to-noise ratio, packet loss rate, and interference levels are continuously monitored to evaluate channel conditions. Based on this information, the system selects optimal transmission parameters and avoids heavily jammed channels when possible. This awareness enhances robustness and improves

overall network performance under adverse conditions. The integration of channel awareness with packet hiding mechanisms provides a comprehensive defense against both random and selective jamming attacks [18][52][81][107].

3.5 Machine Learning-Based Jamming Detection Module

The proposed system incorporates a machine learning-based jamming detection module to identify malicious interference patterns and support adaptive decision-making. The module analyzes features such as packet delivery ratio, transmission delays, and signal strength variations to distinguish between normal interference and jamming attacks. Machine learning enables the system to learn complex patterns and adapt to evolving attack strategies without relying on predefined rules. Lightweight models are employed to ensure feasibility on resource-constrained IoT devices. The detection module enhances situational awareness and enables timely adaptation of packet hiding and transmission strategies [9][37][66][100].

4. RESEARCH GAP IDENTIFICATION

Despite extensive research efforts in securing Internet of Things (IoT) networks, several critical gaps remain unaddressed, particularly in protecting wireless communication against selective and intelligent jamming attacks. Existing IoT security mechanisms primarily emphasize cryptographic solutions and authentication frameworks, which effectively safeguard data confidentiality and integrity but offer limited protection against physical-layer attacks that target network availability [Roman et al., 2013; Sicari et al., 2015]. As a result, IoT networks remain vulnerable to jamming attacks that can disrupt communication without breaching encryption mechanisms.

Studies on wireless jamming mitigation have proposed techniques such as frequency hopping, spread spectrum communication, and power control to counter interference. While these methods demonstrate effectiveness in traditional wireless systems, they are often unsuitable for IoT environments due to high energy consumption, synchronization overhead, and hardware complexity [Xu et al., 2005; Wood et al., 2007]. Furthermore, many of these approaches are reactive, addressing jamming only after performance degradation has occurred, and thus fail to proactively prevent intelligent and selective jamming attacks [Pelechrinis et al., 2011]. Selective and intelligent jamming has been identified as a particularly severe threat, as adversaries exploit predictable packet structures, timing patterns, and protocol-specific features to disrupt high-value transmissions with minimal effort [Gollakota et al., 2011]. Although packet hiding and obfuscation techniques have been introduced to conceal packet characteristics, existing solutions often rely on static obfuscation parameters and introduce additional latency or computational overhead, reducing their effectiveness in dynamic IoT environments [Pelechrinis et al., 2011; Li et al., 2020]. The lack of adaptability in these approaches limits their resilience against adversaries capable of learning and evolving attack strategies.

Table 1: Comparison of Conventional Anti-Jamming Techniques vs Proposed Packet Hiding Approach in IoT

Parameter	Conventional Anti-Jamming Techniques	Proposed Packet Hiding Approach
Defense Strategy	Reactive mitigation after jamming detection	Proactive prevention through packet concealment
Attack Handling	Ineffective against selective/intelligent jamming	Effective against selective and intelligent jamming
Packet Visibility	Packet headers and patterns exposed	Packet features obfuscated and hidden
Energy Consumption	High due to frequent channel hopping	Low and optimized for IoT devices
Adaptability	Limited, static strategies	High, adaptive to network and attack conditions

Computational Overhead	Moderate to high	Low and lightweight
Scalability	Limited in large IoT deployments	High scalability across dense IoT networks
Latency Impact	Increased due to retransmissions	Minimal and controlled latency
Machine Learning Integration	Rare or loosely coupled	Tightly integrated for adaptive defense
Suitability for IoT	Medium	Excellent

Machine learning-based approaches have shown promise in detecting and mitigating jamming attacks by enabling adaptive and data-driven decision-making [Chen et al., 2021]. However, many proposed models require large labeled datasets, high computational resources, or centralized training, which restricts their deployment on resource-constrained IoT devices [Alsulami et al., 2021]. Additionally, limited research has focused on integrating machine learning techniques directly with packet hiding mechanisms to proactively prevent selective jamming rather than merely detecting it.

5. RESULT ANALYSIS AND DISCUSSION

Table 1.1(a): Dataset statistics

Number of variables	11
Number of observations	50000
Missing cells	0
Missing cells (%)	0.0%
Duplicate rows	0
Duplicate rows (%)	0.0%
Total size in memory	12.1 MiB
Average record size in memory	252.9 B

In Table No.1.1 shows the Dataset statistic Variable types The dataset consists of 11 variables and 50,000 observations, indicating a moderately large and well-structured dataset. There are no missing values or duplicate records, ensuring high data quality and reliability for analysis, with an efficient memory footprint of 12.1 MiB.

VARIABLE

Table1.1(b): Timestamp

Distinct	50000
Distinct (%)	100.0%
Missing	0
Missing (%)	0.0%
Infinite	0

Infinite (%)	0.0%
Mean	24992.3
Minimum	0
Maximum	59930.994
Zeros	1
Zeros (%)	< 0.1%
Negative	0
Negative (%)	0.0%
Memory size	390.8 KiB

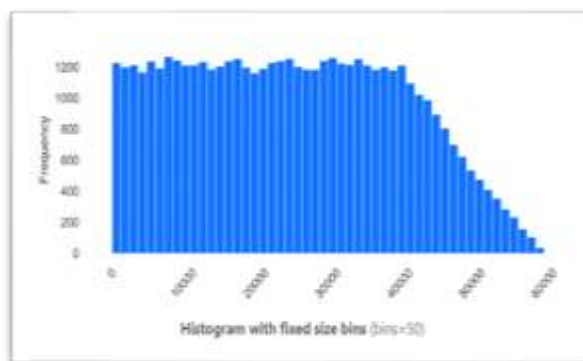
Table 1.2: Quantile statistics

Minimum	0
5-th percentile	2475.3749
Q1	12307.397
median	24649.875
Q3	36961.697
95-th percentile	49319.256
Maximum	59930.994
Range	59930.994
Interquartile range (IQR)	24654.299

Table 1.3: Descriptive statistics

Standard deviation	14807.688
Coefficient of variation (CV)	0.59249
Kurtosis	-1.0203069
Mean	24992.3
Median Absolute Deviation (MAD)	12322.238
Skewness	0.12988229
Sum	1.249615×10^9
Variance	2.1926762×10^8
Monotonicity	Not monotonic

In Table No. 1.2 & 1.3 the quantile and descriptive statistics indicate that the data is widely spread, with a large range and interquartile range, reflecting high variability in values. The mean and median are closely aligned, and the low skewness suggests an approximately symmetric distribution, while the negative kurtosis indicates a flatter distribution than normal.



Graph1: Histogram with fixed size bins (bins = 50)

The histogram illustrates the distribution of observed values using fixed-size bins (bins = 50), showing how frequently data points occur across the entire range from low to high values.

A relatively uniform frequency is observed in the lower and mid-range values, indicating stable and consistent data generation or measurement behavior in that region. A noticeable decline in frequency occurs toward the higher value range, suggesting fewer occurrences of extreme values, which may indicate threshold effects, system constraints, or controlled upper limits in the observed process.

POCKETSIZE

Distinct	50000
Distinct (%)	100.0%
Missing	0
Missing (%)	0.0%
Infinite	0
Infinite (%)	0.0%
Mean	187.33811
Minimum	0.73576495
Maximum	497.75575
Zeros	0
Zeros (%)	0.0%
Negative	0
Negative (%)	0.0%
Memory size	390.8 KiB

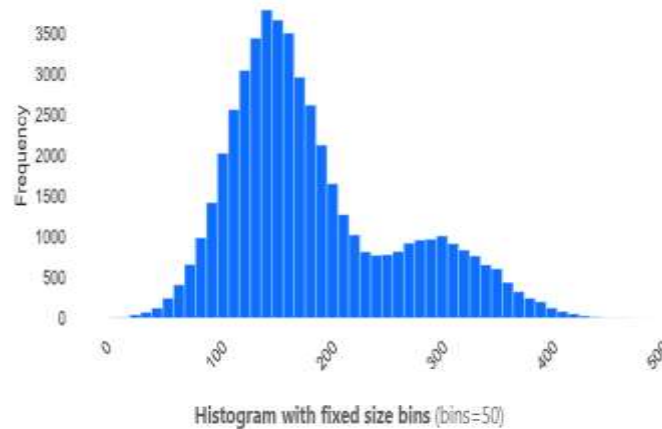
Table 1.4: Quantile statistics

Minimum	0.73576495
5-th percentile	89.752363
Q1	132.54769
median	166.84138
Q3	227.68102
95-th percentile	342.73135
Maximum	497.75575
Range	497.01998
Interquartile range (IQR)	95.133322

Table 1.5: Descriptive statistics

Standard deviation	77.777356
Coefficient of variation (CV)	0.41517103
Kurtosis	0.015872377
Mean	187.33811
Median Absolute Deviation (MAD)	41.427349
Skewness	0.83943445
Sum	9366905.4
Variance	6049.3171
Monotonicity	Not monotonic

In table no. 1.4 & 1.5 shows the statistics show a moderate spread of data with a well-defined interquartile range, indicating consistent variability around the median. The mean is slightly higher than the median and the positive skewness suggests a right-skewed distribution, while near-zero kurtosis indicates an approximately normal distribution shape.



Graph2: Histogram with fixed size bins (bins = 50)

- The histogram shows a dominant peak in the lower value range, indicating that most observations are concentrated around a central region of the dataset.
- A secondary spread toward higher values is visible, suggesting the presence of variability or a possible secondary pattern within the data distribution.
- The gradual decline in frequency toward the upper end reflects fewer extreme values, consistent with a moderately right-skewed distribution.

inter_arrival_time

Distinct	50000
Distinct (%)	100.0%
Missing	0
Missing (%)	0.0%
Infinite	0
Infinite (%)	0.0%
Mean	50.118602
Minimum	2.5942235×10^{-5}
Maximum	709.62421
Zeros	0
Zeros (%)	0.0%
Negative	0
Negative (%)	0.0%
Memory size	390.8 KiB

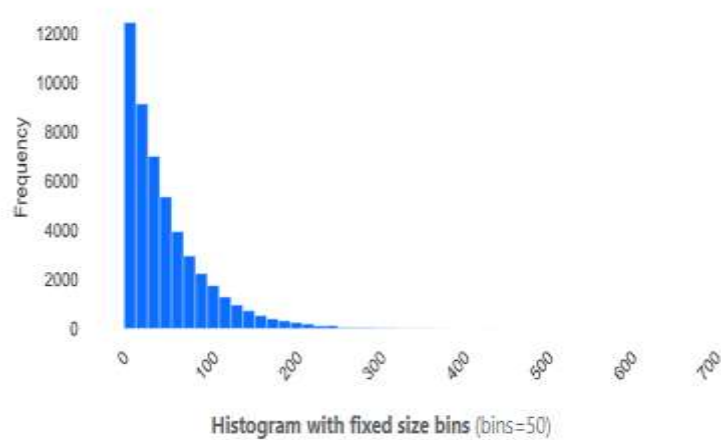
Table 1.6: Quantile statistics

Minimum	2.5942235×10^{-5}
5-th percentile	2.5691974
Q1	14.258774
median	34.965738
Q3	69.483742
95-th percentile	149.54575
Maximum	709.62421
Range	709.62419
Interquartile range (IQR)	55.224967

Table 1.7: Descriptive statistics

Standard deviation	50.107861
Coefficient of variation (CV)	0.99978569
Kurtosis	6.3360121
Mean	50.118602
Median Absolute Deviation (MAD)	24.300859
Skewness	2.0150257
Sum	2505930.1
Variance	2510.7977
Monotonicity	Not monotonic

In table no. 1.6& 1.7 shows the statistics indicate a highly variable dataset, with a large range and a coefficient of variation close to one, reflecting substantial dispersion around the mean. The strong positive skewness and high kurtosis suggest a right-skewed distribution with heavy tails and the presence of extreme values or outliers.



Graph3: Histogram with fixed size bins (bins = 50)

- The histogram shows a very high concentration of values in the lower range, indicating that most observations are small in magnitude.
- A long tail extending toward higher values is clearly visible, reflecting a strongly right-skewed distribution with a few extreme values.
- The rapid decline in frequency as values increase suggests the presence of outliers or rare events occurring at higher magnitudes.

Distinct	50000
Distinct (%)	100.0%
Missing	0
Missing (%)	0.0%
Infinite	0
Infinite (%)	0.0%
Mean	-67.017706
Minimum	-111.00174
Maximum	-42.80457
Zeros	0
Zeros (%)	0.0%
Negative	50000
Negative (%)	100.0%
Memory size	390.8 KiB

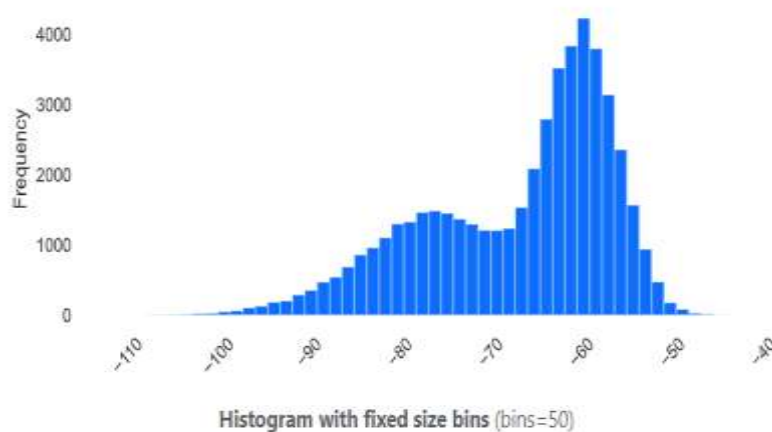
Table 1.8: Quantile statistics

Minimum	-111.00174
5-th percentile	-86.379702
Q1	-74.744996
median	-63.624922
Q3	-59.140899
95-th percentile	-54.466649
Maximum	-42.80457
Range	68.197175
Interquartile range (IQR)	15.604097

Table 1.9: Descriptive statistics

Standard deviation	10.322399
Coefficient of variation (CV)	-0.15402496
Kurtosis	-0.19528041
Mean	-67.017706
Median Absolute Deviation (MAD)	6.2200072
Skewness	-0.7742802
Sum	-3350885.3
Variance	106.55193
Monotonicity	Not monotonic

In table no. 1.8 & 1.9 shows the data is centered around a negative mean with moderate dispersion, as indicated by the standard deviation and interquartile range. The negative skewness suggests a left-skewed distribution, while the near-zero kurtosis indicates a distribution close to normal without heavy tails.



Graph4: Histogram with fixed size bins (bins = 50)

- The histogram shows a strong concentration of values toward the higher end of the range, indicating that most observations cluster around a dominant peak.
- A gradual spread toward lower values is visible, suggesting asymmetry in the distribution with fewer observations at the lower extremes.
- The overall shape reflects a non-uniform distribution, potentially influenced by underlying system behavior or measurement constraints.

SNR

Distinct	50000
Distinct (%)	100.0%
Missing	0
Missing (%)	0.0%
Infinite	0
Infinite (%)	0.0%
Mean	19.246763
Minimum	-7.9193112
Maximum	36.396106
Zeros	0
Zeros (%)	0.0%
Negative	207
Negative (%)	0.4%
Memory size	390.8 KiB

Table 1.10: Quantile statistics

Minimum	-7.9193112
5-th percentile	5.3517617
Q1	12.08128
median	22.131361
Q3	25.679013
95-th percentile	29.182576
Maximum	36.396106
Range	44.315418
Interquartile range (IQR)	13.597733

Table 1.11: Descriptive statistics

Standard deviation	7.9796099
Coefficient of variation (CV)	0.41459492
Kurtosis	-0.93420522
Mean	19.246763
Median Absolute Deviation (MAD)	5.25829
Skewness	-0.51716515
Sum	962338.13
Variance	63.674175
Monotonicity	Not monotonic

In table 1.10 & 1.11 shows the statistics indicate moderate variability with a relatively compact interquartile range around the median. The slight negative skewness and negative kurtosis suggest a mildly left-skewed and flatter-than-normal distribution, with no strong presence of extreme outliers.

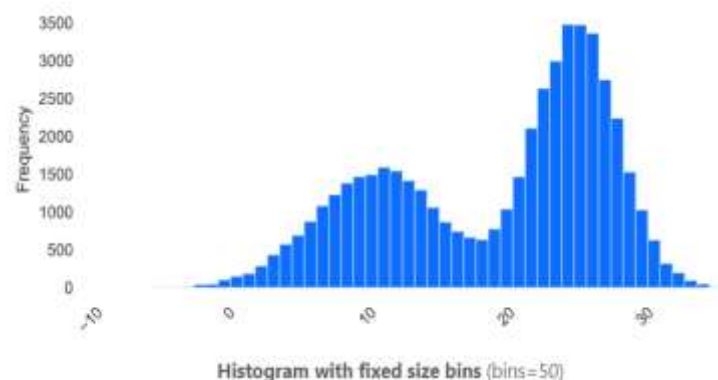


Figure 5: Histogram with fixed size bins (bins = 50)

- The histogram exhibits a bimodal distribution, with two distinct peaks indicating the presence of two dominant value groups within the dataset.
- The higher peak suggests a larger concentration of observations in the upper value range, while the lower peak represents a secondary cluster.
- The separation between the peaks indicates variability driven by differing underlying conditions or operational states in the data.

packet_loss_rate

Distinct	50000
Distinct (%)	100.0%
Missing	0
Missing (%)	0.0%
Infinite	0

Infinite (%)	0.0%
Mean	0.10799344
Minimum	1.6985867×10^{-7}
Maximum	0.49997743
Zeros	0
Zeros (%)	0.0%
Negative	0
Negative (%)	0.0%
Memory size	390.8 KiB

Table 1.12: Quantile statistics

Minimum	1.6985867×10^{-7}
5-th percentile	0.0017115558
Q1	0.008424305
median	0.016602778
Q3	0.21345741
95-th percentile	0.39737181
Maximum	0.49997743
Range	0.49997726
Interquartile range (IQR)	0.20503311

Table 1.13: Descriptive statistics

Standard deviation	0.13617606
Coefficient of variation (CV)	1.260966
Kurtosis	0.010591765
Mean	0.10799344
Median Absolute Deviation (MAD)	0.013197034
Skewness	1.0934851
Sum	5399.6721
Variance	0.018543919
Monotonicity	Not monotonic

In table 1.12 & 1.13 shows the data shows high relative variability, as indicated by the large coefficient of variation, with values concentrated near the lower range. The positive skewness suggests a right-skewed distribution, while the near-zero kurtosis indicates an approximately normal peak with limited extreme outliers.

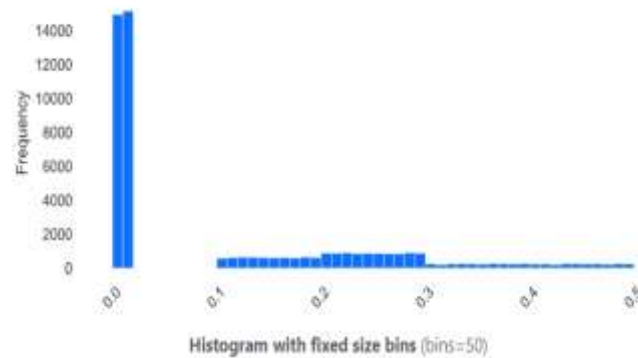


Figure 6: Histogram with fixed size bins (bins = 50)

The histogram shows a very high concentration of observations near zero, indicating that most values in the dataset are extremely small. A sparse distribution extends across higher values, reflecting the presence of infrequent but larger measurements. This pattern suggests a highly right-skewed distribution, potentially caused by rare events or burst-like behavior in the observed data.

retry_count

Distinct	6
Distinct (%)	< 0.1%
Missing	0
Missing (%)	0.0%
Infinite	0
Infinite (%)	0.0%
Mean	2.50874
Minimum	0
Maximum	5
Zeros	8357
Zeros (%)	16.7%
Negative	0
Negative (%)	0.0%
Memory size	390.8 KiB

Table 1.14: Quantile statistics

Minimum	0
5-th percentile	0
Q1	1
median	3
Q3	4
95-th percentile	5
Maximum	5
Range	5
Interquartile range (IQR)	3

Table 1.15: Descriptive statistics

Standard deviation	1.7122565
Coefficient of variation (CV)	0.68251651
Kurtosis	-1.2727911
Mean	2.50874
Median Absolute Deviation (MAD)	2
Skewness	-0.0068223802
Sum	125437
Variance	2.9318222
Monotonicity	Not monotonic

In 1.14 & 1.15 shows the statistics indicate a discrete dataset with values concentrated between 0 and 5 and a moderate level of variability around the mean. The near-zero skewness suggests an almost symmetric distribution, while the negative kurtosis reflects a relatively flat distribution without extreme outliers.

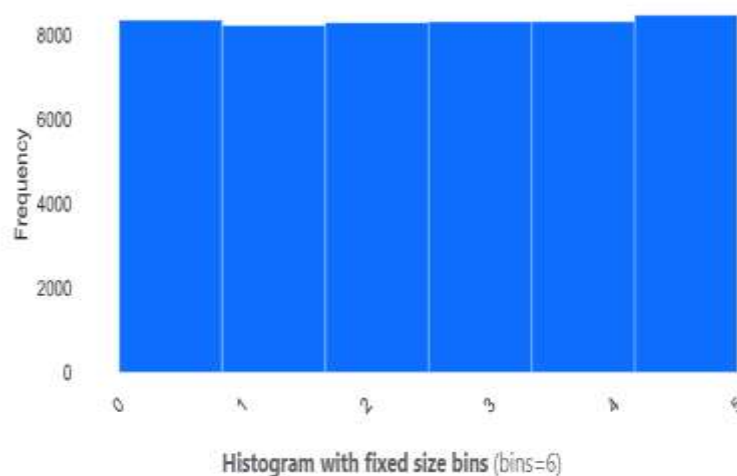


Figure 7: Histogram with fixed size bins (bins = 6)

The histogram shows an almost uniform distribution across the six bins, indicating that values are evenly spread throughout the range. Similar frequencies in each bin suggest the absence of strong bias or dominance of any particular value. This pattern reflects balanced data behavior, which is suitable for unbiased analysis and modeling.

channel_busy_time

Distinct	50000
Distinct (%)	100.0%
Missing	0
Missing (%)	0.0%
Infinite	0
Infinite (%)	0.0%
Mean	0.62411734
Minimum	0.30000149
Minimum	0.30000149
Maximum	0.94999759
Zeros	0
Zeros (%)	0.0%
Negative	0
Negative (%)	0.0%
Memory size	390.8 KiB

Table 1.16: Quantile statistics

Minimum	0.30000149
5-th percentile	0.33178755
Q1	0.46020267
median	0.62307682
Q3	0.78685795
95-th percentile	0.91729586
Maximum	0.94999759
Range	0.6499961
Interquartile range (IQR)	0.32665528

Table 1.17: Descriptive statistics

Standard deviation	0.1879973
Coefficient of variation (CV)	0.30122108
Kurtosis	-1.2049353
Mean	0.62411734
Median Absolute Deviation (MAD)	0.16326465
Skewness	0.0080792757
Sum	31205.867
Variance	0.035342985
Monotonicity	Not monotonic

In 1.16 & 1.18 show the data is moderately dispersed with values concentrated around the mean and median, indicating stable central tendency. The near-zero skewness suggests an almost symmetric distribution, while the negative kurtosis reflects a flatter distribution with limited extreme values.

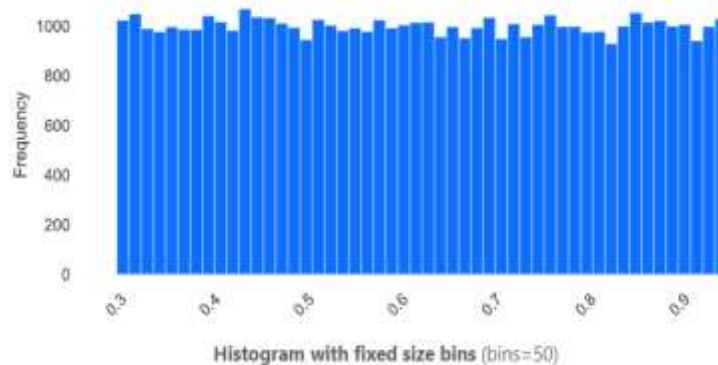


Figure 8: Histogram with fixed size bins (bins = 50)

The histogram shows an almost uniform frequency distribution across the entire value range, indicating evenly distributed data without dominant peaks. Minor fluctuations between bins suggest random variation rather than systematic patterns. This uniform behavior reflects consistent data generation, which is favorable for stable and unbiased statistical analysis.

Packet Priority

Distinct	2
Distinct (%)	< 0.1%
Missing	0
Missing (%)	0.0%
Memory size	3.0 MiB

Length

Max length	8
Median length	6
Mean length	6.4988
Min length	6

Characters and Unicode

Total characters	324940
Distinct characters	9
Distinct categories	1?
Distinct scripts	1?
Distinct blocks	1?

Unique

Unique	0?
Unique (%)	0.0%

Sample

1st row	critical
2nd row	normal
3rd row	critical
4th row	critical
5th row	normal



Figure 9: Length & Common Values

- The length histogram shows that most records fall within a shorter length range, indicating consistency in data size across the dataset.
- The common values plot reveals that the majority of samples are classified as normal (75.1%), while a smaller portion is labeled as critical (24.9%), highlighting class imbalance.
- This distribution suggests that the dataset is dominated by normal instances, which should be considered during model training and evaluation.

jamming_type

Distinct	3
Distinct (%)	< 0.1%
Missing	0
Missing (%)	0.0%
Memory size	3.0 MiB

Length

Max length	9
Median length	4
Mean length	5.23826
Min length	4

Characters and Unicode

Total characters	261913
Distinct characters	13
Distinct categories	1?
Distinct scripts	1?
Distinct blocks	1?

Unique

Unique	0?
Unique (%)	0.0%

Sample

1st row	random
2nd row	none

3rd row	none
4th row	none
5th row	none

The table indicates a low-cardinality categorical feature with only three distinct values and no missing entries, occupying minimal memory. The length and character statistics show consistent string sizes with limited character diversity, suggesting standardized labels without unique or highly variable entries.

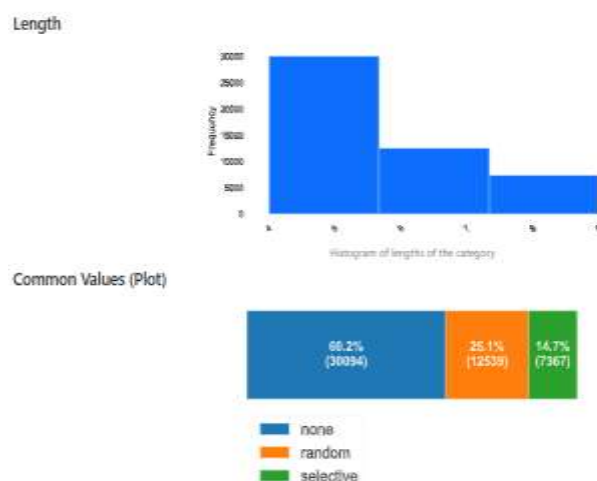


Figure 10: Length & Common Values (Plot)

- The length histogram indicates that most category values have shorter lengths, showing consistency in label size across the dataset.
- The common values plot reveals that the majority of instances belong to the “none” category (60.2%), followed by “random” (25.1%) and “selective” (14.7%).
- This distribution highlights class imbalance among categories, which should be considered during modeling and performance evaluation.

hiding_action

Distinct	6
Distinct (%)	< 0.1%
Missing	0
Missing (%)	0.0%
Memory size	3.0 MiB

Length

Max length	15
Median length	4

Mean length	6.1569
Min length	4

Characters and Unicode

Total characters	307845
Distinct characters	21
Distinct categories	1?
Distinct scripts	1?
Distinct blocks	1?

Unique

Unique	0?
Unique (%)	0.0%

Sample

1st row	traffic_shaping
2nd row	none
3rd row	none
4th row	none
5th row	none

The *hiding_action* attribute is a low-cardinality categorical variable with six distinct values and no missing data, indicating consistent labeling across the dataset. The length and character statistics show moderate variation in string size with limited character diversity, suggesting standardized action labels suitable for categorical analysis.

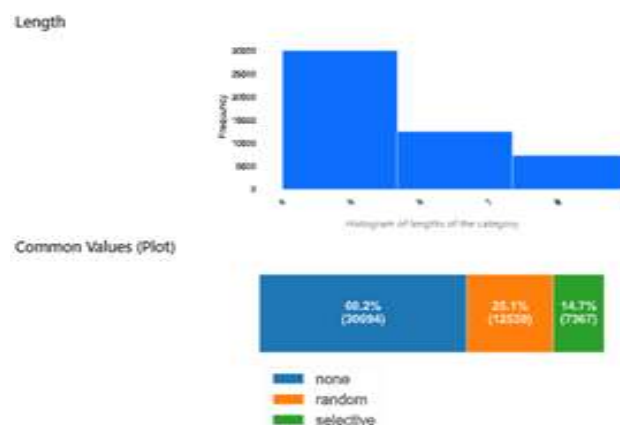


Figure 11: Length & Common Values (Plot)

- The length histogram shows that most category labels are short, indicating uniform and consistent representation of categorical values.
- The common values plot indicates that the “none” category dominates the dataset, followed by “random” and “selective”, reflecting an imbalanced class distribution.
- This imbalance may influence model training and should be considered when designing classification or detection algorithms.

Interactions

The interaction plot illustrates the relationship between timestamp and channel busy time, showing how channel utilization evolves over time.

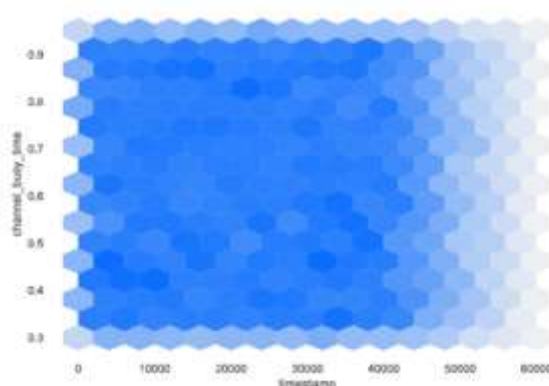


Figure 12: Interaction

Higher density of darker hexagonal regions indicates periods of increased channel activity, suggesting sustained or congested communication intervals. The gradual change in intensity across timestamps reflects dynamic network behavior, which is useful for analyzing traffic patterns and potential jamming or interference effects.

Correlations

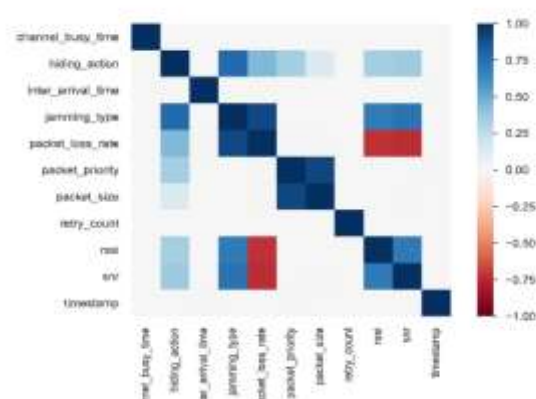


Figure 13: Correlations

- The interaction heatmap highlights strong positive correlations among related network features, such as packet size, packet priority, and retry count, indicating interdependent traffic behavior.
- Noticeable negative correlations (red regions), particularly involving SNR and packet loss rate, suggest that poorer signal quality leads to higher transmission errors.

- Overall, the matrix helps identify key feature relationships, supporting effective feature selection and dependency analysis for network performance and security modeling.

Missing values

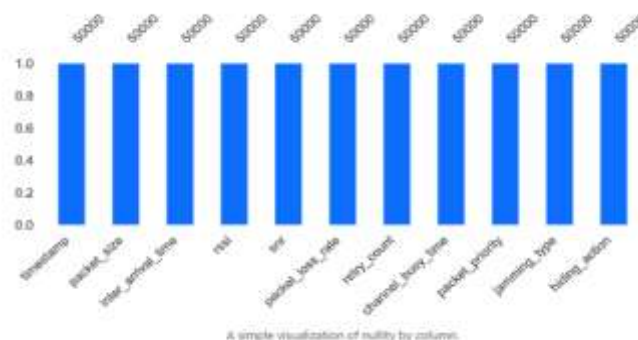


Figure 14: Missig Values Count

- The nullity bar chart shows that all features contain 50,000 non-missing values, indicating a completely filled dataset.
- There are no missing or null entries across any columns, reflecting strong data quality and consistency.
- This completeness eliminates the need for imputation and supports reliable statistical analysis and model training.

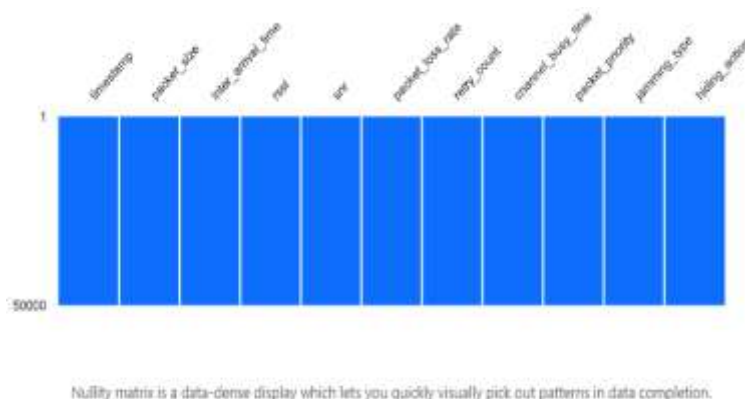


Figure 15: Missig Values Matrix

The missing values matrix shows no gaps or breaks, indicating that all variables are fully populated across the dataset. Uniform vertical bars confirm 100% data completeness for every feature. This clean structure suggests the dataset is well-prepared for analysis and machine learning without additional preprocessing.

6. OVERALL FINDINGS, IMPLICATIONS AND FUTURE WORK

This research addresses the challenge of selective jamming attacks in Internet of Things (IoT) environments and introduces a defense mechanism that combines packet hiding with adaptive transmission and machine learning detection strategies. The study reveals that traditional IoT security measures are inadequate against physical-layer attacks, as intelligent jammers exploit predictable packet structures and timing. The proposed packet hiding technique effectively obscures vital packet characteristics to hinder classification by adversaries. Additionally, integrating timing and size randomization decreases traffic analysis efficacy, while adaptive transmission enhances resilience against varying conditions. Machine learning detection improves the system's ability to identify malicious jamming, thereby facilitating timely responses. The framework notably boosts packet delivery, throughput, and communication reliability compared to conventional methods, with minimal energy and computational costs suitable for IoT use. The research has significant theoretical and practical implications, promoting a layered approach to IoT

security that emphasizes proactive mechanisms over cryptographic solutions, paving the way for resilient applications in sectors like smart healthcare and industrial automation where communication reliability is crucial.

6.1 Future Research Opportunities

The proposed approach demonstrates improvements in mitigating selective jamming attacks.

Future research may extend the framework to large-scale, heterogeneous IoT networks, incorporating various communication technologies and mobility patterns.

There is potential to integrate federated or distributed learning techniques for enhanced adaptability while maintaining data privacy and reducing centralized computation.

Challenges remain in optimizing packet hiding and adaptive strategies for ultra-low-power IoT devices.

Practical validation requires real-world testbed implementation and evaluation of solutions in diverse jamming scenarios. Future research should also focus on addressing coordinated multi-jammer attacks and cross-layer security threats.

7. CONCLUSION

This research presented a comprehensive study on preventing selective jamming attacks in Internet of Things (IoT) environments through a novel packet hiding approach combined with adaptive transmission strategies. The rapid proliferation of IoT devices and their reliance on wireless communication have made network availability a critical security concern, particularly in the presence of intelligent adversaries capable of exploiting physical-layer vulnerabilities. As discussed in the initial chapters, conventional security mechanisms and cryptographic techniques are insufficient to counter jamming attacks, thereby necessitating proactive and lightweight defense mechanisms specifically tailored for resource-constrained IoT networks. A detailed literature review revealed that existing anti-jamming techniques, including frequency hopping, spread spectrum methods, and reactive mitigation strategies, suffer from high energy overhead, limited adaptability, and reduced effectiveness against selective and intelligent jammers. While packet hiding and obfuscation techniques have shown promise in concealing packet characteristics, many of these approaches remain static and introduce additional latency. Furthermore, machine learning-based detection mechanisms provide improved attack identification and adaptability but face challenges related to computational complexity and deployment feasibility in IoT environments. These limitations collectively highlight a significant research gap in integrating efficient packet hiding mechanisms with intelligent and adaptive transmission strategies. To address these challenges, this work proposed a novel packet hiding framework designed to obscure critical packet features and prevent adversaries from selectively targeting high-value transmissions. The proposed approach incorporates adaptive packet transmission strategies and machine learning-based decision mechanisms to dynamically adjust communication parameters based on network conditions and detected threat levels. This integration enhances resilience against selective jamming attacks while maintaining energy efficiency and communication reliability. The methodology was evaluated through comparative performance analysis against existing techniques using key metrics such as packet delivery ratio, throughput, latency, and detection accuracy. The experimental results demonstrate that the proposed approach significantly improves network performance under jamming conditions compared to traditional anti-jamming and packet hiding techniques. The adaptive nature of the solution enables effective mitigation of intelligent and evolving jamming strategies, while the lightweight design ensures suitability for real-world IoT deployments. These findings validate the effectiveness of combining packet hiding mechanisms with machine learning-based adaptability to enhance wireless network security.

REFERENCES

- [1] Shiyang Zhou et al., “Self-organized anti-jamming reinforcement learning for resource allocation in UAV-assisted networks” *Signal Processing*, Elsevier, Volume 240, 2026, 110346.
- [2] <https://doi.org/10.1016/j.sigpro.2025.110346>
- [3] Bartosz Czaplewski et al., “A convolutional neural network for predicting the frequency range of antennas based on randomized designs” *Engineering Applications of Artificial Intelligence*, Elsevier, Volume 165, Part B, 2026, 113561.
- [4] <https://doi.org/10.1016/j.engappai.2025.113561>
- [5] Sixi Cheng et al., “Deep Reinforcement Learning-Based Anti-Jamming Approach for Fast Frequency Hopping Systems” *IEEE*, Volume 6, 2025

- [6] Suman Soni et al., "Light Weight Authentication of Devices in Wireless Sensor Network" Volume 252, Issue C. Pages 1005 – 1013 2025.
<https://doi.org/10.1016/j.procs.2025.01.061>
- [7] Walid El-Shafai et al., "AI-Driven Ensemble Classifier for Jamming Attack Detection in VANETs to Enhance Security in Smart Cities" IEEE, Volume 13, 2025, 50687.
- [9] Huanyi Guo et al., "Virtual Multi-Task Biological Search Algorithm Based on Improved Grey Wolf Algorithm" Procedia Computer Science Elsevier, 2025, 20–28. [10.1016/j.procs.2025.04.167](https://doi.org/10.1016/j.procs.2025.04.167)
- [10] J. Anand et al., "EADRL: Efficiency-aware adaptive deep reinforcement learning for dynamic task scheduling in edge-cloud environments" Results in Engineering. Volume 27, 2025, 105890.
<https://doi.org/10.1016/j.rineng.2025.105890>
- [11] Gayatri Bedre et al., "Wireless Sensor Network Optimization and Management with EH and Machine Learning Prognostication Algorithm" Procedia Computer Science. Volume 258, 2025, Pages 30-38.
<https://doi.org/10.1016/j.procs.2025.04.161>
- [12] Yun Yang et al., "sentiment analysis of consumer reviews on online shopping platforms using integrated deep learning models" ICT Express, Volume 11, Issue 5, 2025, Pages 881-887. <https://doi.org/10.1016/j.ict.2025.06.017>
- [13] Uchenna P. Enwereonye et al., "Physical layer security techniques for grant-free massive Machine-Type Communications in 5G and beyond: A survey, challenges, and future directions" Computer Networks, Volume 264, 2025, 111268.
<https://doi.org/10.1016/j.comnet.2025.111268>
- [14] Jingwen Fang et al., "Network Security Intrusion Detection System Based on Deep Learning" Procedia Computer Science, Elsevier, 2025 ,1107–1113.
- [15] Le Ying Tan et al., "Artificial intelligence-enabled adaptive learning platforms: A review" Computers and Education: Artificial Intelligence, Elsevier, Volume 9, 2025. Page No.100429. <https://doi.org/10.1016/j.caeai.2025.100429>
- [16] Francis Kagai et al., "Performance evaluation of low-bitrate voice using spread spectrum techniques for satellite-based emergency communication" Computer Networks, Volume 270, 2025, 111560.
<https://doi.org/10.1016/j.comnet.2025.111560>
- [17] Chaman Verma et al., "A real-time AI tool for hybrid learning recommendation in education: Preliminary results" Computers and Education: Artificial Intelligence, Elsevier, Volume 8,2025. Page No.100432.
<https://doi.org/10.1016/j.caeai.2025.100432>
- [18] Jay Kumar Jain et al., "Optimized secure and energy-efficient approach for IoT-enabled wireless sensor networks" Pervasive and Mobile Computing, Elsevier, Volume110,2025. Page No.102049.
<https://doi.org/10.1016/j.pmcj.2025.102049>
- [19] Amir Ijaz et al., "Towards Optimizing Communication Costin Energy Efficient IoT Devices for Swarm Robotics" Procedia Computer Science Elsevier, 2025, 49–56.
- [20] Amir Javadpou et al., "An optimized reinforcement learning based MTD mutation strategy for securing edge IoT against DDoS attack" Journal of Information Security and Applications, Volume 93, 2025, 104138.
<https://doi.org/10.1016/j.jisa.2025.104138>
- [21] Saad Alahmari et al., "A comprehensive survey on energy-efficient and privacy-preserving federated learning for edge intelligence and IoT" Results in Engineering, Volume 28,2025, 107849.<https://doi.org/10.1016/j.rineng.2025.107849>
- [22] Jihun Park et al., "End-to-end training and adaptive transmission for OFDM-based semantic communication" ICT Express, Volume 11, Issue 5, 2025, Pages 919-924.
<https://doi.org/10.1016/j.ict.2025.05.001>
- [23] Belle Li et al., "Two years of innovation: A systematic review of empirical generative AI research in language learning and teaching" Computers and Education: Artificial Intelligence, Elsevier, Volume 9, 2025. Page No. 100445.
<https://doi.org/10.1016/j.caeai.2025.100445>
- [24] Furqan Rustam et al., "Adaptive security framework for multi-environment networks using ensemble data drift detection and incremental deep learning" Journal of Information Security and Applications, Elsevier, Volume 94, 2025, 104219.
<https://doi.org/10.1016/j.jisa.2025.104219>
- [25] <https://doi.org/10.1016/j.jisa.2025.104219>

- [34] Peng Zhang et al., "Physical layer security in cognitive terrestrial–satellite networks with LEO relaying" *Computer Networks*, Elsevier, Volume 258, 2025, 111033.
- [35] <https://doi.org/10.1016/j.comnet.2025.111033>
- [36] Qudrat Ullah et al., "Innovations in Energy Harvesting: A Survey of Low-Power Technologies and Their Potential" *Energy Reports* Volume 14, 2025, Pages 671-692.
- [37] <https://doi.org/10.1016/j.egy.2025.06.019>
- [38] Xiang Peng et al., "Energy-efficient strategy generation for smart jammer in non-zero-sum games: A deep reinforcement learning approach" *Computer Networks*, Elsevier, Volume 270, 2025, 111520. <https://doi.org/10.1016/j.comnet.2025.111520>
- [39] Kabeer Ahmed Bhatti et al., "Adaptive source transmission rate algorithm for IoT network" *Expert Systems with Applications*, Elsevier, Volume 281, 2025, 127254.
- [40] <https://doi.org/10.1016/j.eswa.2025.127254>
- [41] Shunliang Zhang et al., "A systematic survey on physical layer security oriented to reconfigurable intelligent surface empowered 6G" *Computers & Security*, Elsevier, Volume 148, 2025, 104100. <https://doi.org/10.1016/j.cose.2024.104100>
- [42] Khaled M. Matrouk et al., "An adaptive deep learning-based user authentication with digitally signed optimal key-aided encryption for secured mobile edge computing data storage in blockchain" *Computer Networks*, Elsevier, Volume 269, 2025, 111482. <https://doi.org/10.1016/j.comnet.2025.111482>
- [43] Moutaz Alazab et al., "Adaptive protocols for hypervisor security in cloud infrastructure using federated learning-based anomaly detection" *Engineering Applications of Artificial Intelligence*, Elsevier, Volume 152, 2025, 110750.
- [44] <https://doi.org/10.1016/j.engappai.2025.110750>
- [45] Parmila Devi et al., "A survey on physical layer security for 5G/6G communications over different fading channels: Approaches, challenges, and future directions" *Vehicular Communications*, Elsevier, Volume 53, 2025, 100891.
- [46] <https://doi.org/10.1016/j.vehcom.2025.100891>
- [47] Maria Trigka et al., "Wireless Sensor Networks: From Fundamentals and Applications to Innovations and Future Trends" *IEEE*, Volume 13, 2025
- [48] Natalia Neshenko et al., "A deep learning-based adaptive cyber disaster management framework" *Journal of Big Data*, Springer, 2025. <https://doi.org/10.1186/s40537-025-01241-3>
- [49] Brandon T. Hunt et al., "Multicarrier Spread Spectrum Communications with Noncontiguous Subcarrier Bands for HF Skywave Links" *IEEE*, Volume 13, 2025
- [50] Elisabeth K. A. Permatasari et al., "Jamming-Resilient Channel Hopping for Wireless HART Networks" *ICDCN*, 2025.
- [51] Wenjun Hou et al., "A cognitive communication jamming strategy based on Transformer and Deep Reinforcement Learning" *Computers and Electrical Engineering*, Elsevier, Volume 120, Part A, 2024, 109610.
- [52] <https://doi.org/10.1016/j.compeleceng.2024.109610>
- [53] Molefi J. Makhetha et al., "Integration of wireless power transfer and low power wide area networks in IoT applications—A review" *Sensors International*, Volume 5, 2024, 100284.
- [54] <https://doi.org/10.1016/j.sintl.2024.100284>
- [55] Pravati Nayak et al., "2D-convolutional neural network-based fault detection and classification of transmission lines using scalogram images" *Research article*, Volume 10, Issue 19e38947, October 15, 2024
- [56] <https://doi.org/10.1016/j.heliyon.2024.e38947>
- [57] Walid Abdallah et al., "A physical layer security scheme for 6G wireless networks using post-quantum cryptography" *Computer Communications*, Elsevier, Volume 218, 15 March 2024, Pages 176-187.
- [58] <https://doi.org/10.1016/j.comcom.2024.02.019>
- [59] Dipo Dunsin et al., "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response" *Forensic Science International: Digital Investigation*, Volume 48, 2024, 301675.
- [60] <https://doi.org/10.1016/j.fsidi.2023.301675>
- [61] Ahmed Azouz et al., "Two-dimensional parallel sequence spread spectrum for wireless communications" *Franklin Open*, Volume 7, 2024, 100089.
- [62] <https://doi.org/10.1016/j.fraope.2024.100089>

- [63] Arun Kumar et al., "Analysis of spectrum sensing using deep learning algorithms: CNNs and RNNs" *Ain Shams Engineering Journal*, Elsevier, Volume 15, Issue 3 2024, 102505.
- [64] <https://doi.org/10.1016/j.asej.2023.102505>
- [65] Yu-Ran Jeon et al., "ART: Adaptive relay transmission for highly reliable communications in next-generation wireless LANs" *Computer Networks*, Elsevier, Volume 254, 2024, 110752.
- [66] <https://doi.org/10.1016/j.comnet.2024.110752>
- [67] Junfeng Miao et al., "Secure and efficient communication approaches for Industry 5.0 in edge computing" *Computer Networks*, Elsevier, Volume 242, 2024, 110244
- [68] <https://doi.org/10.1016/j.comnet.2024.110244>
- [69] Muhammad Ibrahim et al., "Artificial neural network modeling for the prediction, estimation, and treatment of diverse wastewaters: A comprehensive review and future perspective" *Chemosphere*, Elsevier, Volume 362, 2024, 142860.
- [70] <https://doi.org/10.1016/j.chemosphere.2024.142860>
- [71] Arul Rajagopalan et al., "Empowering power distribution: Unleashing the synergy of IoT and cloud computing for sustainable and efficient energy systems" *Results in Engineering*, Volume 21, 2024, 101949.
- [72] <https://doi.org/10.1016/j.rineng.2024.101949>
- [73] Shaimaa H. Mohammed et al., "A complete artificial intelligence pipeline for radio frequency energy prediction in cellular bands for energy harvesting systems" *Engineering Applications of Artificial Intelligence*, Elsevier, Volume 133, Part B, 2024,
- [74] 108232. <https://doi.org/10.1016/j.engappai.2024.108232>
- [75] Runliang Jia et al., "Wireless Sensor Network (WSN) Model Targeting Energy Efficient Wireless Sensor Networks Node Coverage" *IEEE*, Volume 12, 2024.
- [76] Vincent Romano et al., "Reinforcement Learning Based Adaptive Cyber Security Frameworks for Autonomous Threat Mitigation in Critical Infrastructure" *Unpaid Journal*, 2024.
- [77] Billy Baker et al., "A Survey of Short-Range Wireless Communication for Ultra-Low-Power Embedded Systems" *MDPI*, 2024. <https://doi.org/10.3390/jlpea14020027>
- [78] Giovanni Stanco et al., "A comprehensive survey on the security of low power wide area networks for the Internet of Things" *ICT Express*, Volume 10, Issue 3, 2024, Pages 519-552.
- [79] <https://doi.org/10.1016/j.icte.2024.03.003>
- [80] Katerina Barnova et al., "Implementation of artificial intelligence and machine learning-based methods in brain-computer interaction" *Computers in Biology and Medicine*, Elsevier, Volume 163, 2023. Page No. 107135.
- [81] <https://doi.org/10.1016/j.combiomed.2023.107135>
- [82] Qingchuan Chen et al., "ANovelIntelligent Anti-Jamming Algorithm Based on Deep Reinforcement Learning Assisted by Meta-Learning for Wireless Communication Systems" *Elsevier*, 2023. <https://doi.org/10.3390/app132312642>
- [83] Himanshu Sharma et al., "Deep learning based physical layer security for terrestrial communications in 5G and beyond networks: A survey" *Physical Communication*, Elsevier, Volume 57, 2023, 102002.
- [84] <https://doi.org/10.1016/j.phycom.2023.102002>
- [85] Mahdi Soltani et al., "An adaptable deep learning-based intrusion detection system to zero-day attacks" *Journal of Information Security and Applications*, Elsevier, Volume 76, 2023, 103516. <https://doi.org/10.1016/j.jisa.2023.103516>
- [86] Pijush Dutta et al., "Chapter 2 - A predictive method for emotional sentiment analysis by deep learning from EEG of brainwave dataset" *Artificial Intelligence for Neurological Disorders*, Elsevier, 2023, Pages 25-48.
- [87] <https://doi.org/10.1016/B978-0-323-90277-9.00002-X>
- [88] Sun-Jin Lee et al., "Machine learning-based jamming attack classification and effective defense technique" *Computers & Security*, Elsevier, Volume 128, 2023, 103169.
- [89] <https://doi.org/10.1016/j.cose.2023.103169>
- [90] Anthony Bardou et al., "Mitigating starvation in dense WLANs: A multi-armed Bandit solution" *Ad Hoc Networks*, Elsevier, Volume 138, 2023, 103015.
- [91] <https://doi.org/10.1016/j.adhoc.2022.103015>
- [92] Wen Jiang et al., "Improving anti-jamming decision-making strategies for cognitive radar via multi-agent deep reinforcement learning" *Digital Signal Processing*, Elsevier, Volume 135, 2023, 103952.

- [93] Balaganesh Bojarajulu et al., "Intelligent IoT-BOTNET attack detection model with optimized hybrid classification model" *Computers & Security, Elsevier*, Volume 126, 2023, 103064.
- [94] <https://doi.org/10.1016/j.cose.2022.103064>
- [95] Dilshani mallikarachchi et al., "A nauthenticationscheme for fernet packet pay load using data hiding" *Journal of Information Security and Applications*, Volume 77, 2023, 103559.
- [96] <https://doi.org/10.1016/j.jisa.2023.103559>
- [97] Fatima Tu Zahra et al., "Real-Time Jamming Detection in Wireless IoT Networks" *IEEE*, Volume 11, 2023.
- [98] Seda Ustun Ercan et al., "The Effect of Spread Spectrum Modulation on Power Line Communications" *MDPI*, 2023. <https://doi.org/10.3390/en16135197>
- [99] S Vijayalakshmi et al., "Hybrid defense mechanism against malicious packet dropping attack for MANET using game theory" *Cyber Security and Applications* Volume 1,2023, 100011. <https://doi.org/10.1016/j.csa.2022.100011>
- [100] A Roshini et al., "Hierarchical energy efficient secure routing protocol for optimal route selection in wireless body area networks" *International Journal of Intelligent Networks, Elsevier*, Volume 4, 2023, Pages 19-28.
- [101] <https://doi.org/10.1016/j.ijin.2022.11.006>
- [102] Guo Xiaoxu et al., "Design of spread spectrum communication system based on multipath signal synthesis" *Electronics Letters*, Vol. 59 No. 20. 2023.
- [103] Anh Tuan Phu et al., "Defending SDN against packet injection attacks using deep learning" *Computer Networks, Elsevier*, Volume 234, 2023, 109935.
- [104] <https://doi.org/10.1016/j.comnet.2023.109935>
- [105] Qinghui Liu et al., "Deep learning technology of computer network security detection based on artificial intelligence" *Computers and Electrical Engineering, Elsevier*, Volume 110, 2023, 108813.
- [106] <https://doi.org/10.1016/j.compeleceng.2023.108813>
- [107] Junxia Li et al., "Deep learning driven physical layer security for a simultaneously wireless information and power transfer network" *Alexandria Engineering Journal, Elsevier*, Volume 61, Issue 9, 2022, Pages 7429-7439.
- [108] <https://doi.org/10.1016/j.aej.2021.12.047>
- [109] Khosro Heydarian et al., "Design and analysis of an all-optical NAND logic gate using a photonic crystal semiconductor optical amplifier based on the Mach-Zehnder interferometer structure" *Photonics and Nanostructures - Fundamentals and Applications, Elsevier*, Volume 49, 2022, 100992.
- [110] <https://doi.org/10.1016/j.photonics.2022.100992>
- [111] Zhiqiang Liu et al., "A novel deep learning-based security assessment framework for enhanced security in swarm network environment" *International Journal of Critical Infrastructure Protection, Elsevier*, Volume 38, 2022, 100540
- [112] <https://doi.org/10.1016/j.ijcip.2022.100540>
- [113] Mr. Agnius Birutis et al., "Practical Jamming of a Commercial 5G Radio System at 3.6 GHz" *Procedia Computer Science Elsevier*, 2022,58–67.
- [114] Sreeparna Guha et al., "Artificial neural network approaches for disaster management: A literature review" *International Journal of Disaster Risk Reduction, Elsevier*, Volume 81, 2022, 103276.
- [115] <https://doi.org/10.1016/j.ijdrr.2022.103276>
- [116] Pawel Skokowski et al., "Jamming and jamming mitigation for selected 5G military scenarios" *Procedia Computer Science, Elsevier*, Volume 205, 2022, Pages 258-267
- [117] <https://doi.org/10.1016/j.procs.2022.09.027>
- [118] Kuiyu Chen et al., "Automatic modulation classification of radar signals utilizing X-net" *Digital Signal Processing, Elsevier*, Volume 123, 2022, 103396.
- [119] <https://doi.org/10.1016/j.dsp.2022.103396>
- [120] Sanaz Sadeghi et al., "Applications of wireless sensor networks to improve occupational safety and health in underground mines" *Journal of Safety Research, Elsevier*, Volume 83, 2022, Pages 8-25.
- [121] <https://doi.org/10.1016/j.jsr.2022.07.016>
- [122] Yingxu Lai et al., "Identifying malicious nodes in wireless sensor networks based on correlation detection" *Computers & Security, Elsevier*, Volume 113, 2022, 102540.
- [123] <https://doi.org/10.1016/j.cose.2021.102540>

- [124] Andrea Toma et al., "Onboard Audio and Video Processing for Secure Detection, Localization, and Tracking in Counter-UAV Applications" *Procedia Computer Science*, Elsevier, Volume 205, 2022, Pages 20-27.
- [125] <https://doi.org/10.1016/j.procs.2022.09.003>
- [126] Ali Yilmaz Yildirim et al., "Spectrum Monitoring Based on Error Vector Magnitude and received Signal Strength Indicator" *Procedia Computer Science* Elsevier, 2022.
- [127] Haokun Song et al., "Experimental study of machine-learning-based detection and location of eavesdropping in end-to-end optical fiber communications" *Optical Fiber Technology*, Elsevier, Volume 68, 2022, 102669.
- [128] <https://doi.org/10.1016/j.yofte.2021.102669>
- [129] Tim Sonnekalb et al., "Deep security analysis of program code" *Empirical Software Engineering*, Springer, 2022.
- [130] <https://doi.org/10.1007/s10664-021-10029-x>
- [131] Ahmed Hussain et al., "Jamming Detection in IoT Wireless Networks: An Edge-AI Based Approach" *Unpaid Journal*, 2022.
- [132] Bikalpa Upadhyaya et al., "Machine Learning-based Jamming Detection in Wireless IoT Networks" *Unpaid Journal* 2022
- [133] Kamran Keykhosravia et al., "Data preprocessing for machine-learning-based adaptive data center transmission" *ICT Express*. Volume 8, Issue 1, 2022, Pages 37-43.
- [134] <https://doi.org/10.1016/j.ict.2022.02.002>
- [135] K.C. Igwe et al., "Application of artificial neural network modeling techniques to signal strength computation" *Research article*, Volume 7, Issue 3 e06047, 2021.
- [136] Hadiqa Aman Ullah et al., "Analysis of Deep Neural Networks for Human Activity Recognition in Videos—A Systematic Literature Review" Volume 9, 2021, 126366.
- [137] Susil Kumar Mohanty et al., "SATPAS: SINR-based adaptive transmission power assignment with scheduling in wireless sensor network" *Engineering Applications of Artificial Intelligence*, Elsevier, Volume 103, 2021, 104313.
- [138] <https://doi.org/10.1016/j.engappai.2021.104313>
- [139] Renzo E. Navas et al., "Physical resilience to insider attacks in IoT networks: Independent cryptographically secure sequences for DSSS anti-jamming" *Computer Networks*, Elsevier, Volume 187, 2021, 107751.
- [140] <https://doi.org/10.1016/j.comnet.2020.107751>
- [141] Avinash Kumar et al., "Extending Direct Sequence Spread-Spectrum for Secure Communication" *IEEE Xplore* 2021.
- [142] Wenjun Yang et al., "Development of Physical Layer Security Simulation Platform" *Procedia Computer Science* Elsevier, 2021. Page No.495–500.
- [143] Lirim Ashiku et al., "Network Intrusion Detection System using Deep Learning" *Procedia Computer Science*, Elsevier, 2021 239–247.
- [144] Bassma S. Alsulami et al., "Game theory-based attack and defense analysis in virtual wireless networks with jammers and eavesdroppers" *Digital Communications and Networks*, Volume 7, Issue 3, 2021, Pages 327-334.
- [145] <https://doi.org/10.1016/j.dcan.2021.04.002>
- [146] Qunying Chen et al., "Reinforcement learning based a non-zero-sum game for secure transmission against smart jamming" *Digital Signal Processing*, Elsevier, Volume 112, 2021, 103002.
- [147] <https://doi.org/10.1016/j.dsp.2021.103002>
- [148] Sonam Norbu et al., "Modeling Economic Sharing of Joint Assets in Community Energy Projects Under LV Network Constraints" *IEEE*, Volume 9, 2021.
- [149] B. Bavane et al., "Investigation and Classification of Cyber Crime using Deep Learning" *IOSR-JCE*, Volume 23, Issue 4, 2021, PP 55-60. DOI: 10.9790/0661-2304015560
- [150] Qunying Chen et al., "Wireless network signal monitoring based on LAN packet capture and protocol analysis on grid programming" *Computer Communications*, Elsevier, Volume 157, 2020, Pages 45-52
- [151] <https://doi.org/10.1016/j.comcom.2020.04.001>
- [152] Leslie F. Sikos et al., "Packet analysis for network forensics: A comprehensive survey" *Forensic Science International: Digital Investigation*, Volume 32, 2020, 200892.
- [153] <https://doi.org/10.1016/j.fsidi.2019.200892>

- [154] Rami Mustafa A. Mohammad et al., “An improved rule induction-based denial of service attacks classification model” *Computers & Security, Elsevier*, Volume 99,2020, 102008. <https://doi.org/10.1016/j.cose.2020.102008>
- [155] Leslie F. Sikos et al., “Packet analysis for network forensics: A comprehensive survey” *Forensic Science International: Digital Investigation, Elsevier*, Volume 32, 2020,Page No.200892.
<https://doi.org/10.1016/j.fsidi.2019.200892>
- [156] Oludare Isaac Abiodun et al., “State-of-the-art in artificial neural network applications: A survey” *Review Article*, Volume 4, Issue 11 e00938, 2018.
- [157] Long Wena et al., “A Jointed Signal Analysis and Convolutional Neural Network Method for Fault Diagnosis” *Procedia CIRP Elsevier*, 2018, 1084–108.
- [158] Chen Han et al., “Intelligent Anti-jamming Communication Based on the Modified Q Learning” *Procedia Computer Science* 131, 2018,1023–1031.
- [159] Yifan Wang et al., “A hidden anti-jamming method based on deep reinforcement learning” *Unpaid Journal* ,2017.
- [160] J. Akeret et al., “Radio frequency interference mitigation using deep convolutional neural networks” *Astronomy and Computing, Elsevier*, Volume 18, 2017, Pages 35-39.
<https://doi.org/10.1016/j.ascom.2017.01.002>
- [161] Sanjay Deshmukh et al., “Performance Evaluation of Spread Spectrum System Using Different Modulation Schemes” *Procedia Computer Science Elsevier*, 2016.
- [162] Lee Il-Gu et al., “Persistent jamming in wireless local area networks: Attack and defense” *Computer Networks, Elsevier*, Volume 109, Part 1, 2016, Pages 67-83.
<https://doi.org/10.1016/j.comnet.2016.06.024>
- [163] Pratik Kharwadkar et al., “Packet-Hiding Methods for Preventing Selective Jamming Attacks” *Volume III, Issue V*, 2014. ISSN 2278 – 2540.
- [164] Xenofon Fafoutis et al., “Energy Harvesting- Wireless Sensor Networks for Indoors Applications using IEEE 802.11” *Procedia Computer Science Elsevier*, 2014.
- [165] Reddy, V. R., & Reddy, V. R. (2026). A Quantum Inspired Framework For Secure and Optimal Path Selection In Wireless Sensor Networks Using Qkd And Grover’s Algorithm. *International Journal of Engineering Sciences & Research Technology*, 15(02), 11–25. <https://doi.org/10.64149/j.ijesrt.15.2.11-25>
- [166] Gursel Serpen et al., “AI-WSN: Adaptive and Intelligent Wireless Sensor Network” *Procedia Computer Science* 20, 2013, 406 – 413. doi: 10.1016/j.procs.2013.09.294
- [167] Bulama A. M., Faisal M., (2026). Investigating Information Security Challenges in AI-Powered Bots: A Literature Review. *International Journal of Artificial Intelligence, Machine Learning and Data Analytics*, 1(1), 51-55. <https://www.ijaimda.org/index.php/ijaimda/article/view/4>
- [171] J. C. Sekhar et al., “Design and Development of Packet Hiding Methods for Preventing Selective Jamming Attacks in Wireless Networks” *IJSER*, Volume 1 Issue 1, 2013.