Journal of Trends in Computer Science and Smart Technology (ISSN: 2582-4104)
www.irojournals.com/tcsst/

Adversarial Attack Detection in Wireless Networks Using Deep Learning Based Capsule Networks

Sneha George[1], Priscilla Joy R.[2], Karuppasamy K.[3]

[1,2]Division of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, India.
[3]Department of Computer Science and Engineering, RVS College of Engineering and Technology, Sulur, Coimbatore, India.

E-mail: [1]snehageorge2724@gmail.com, [2]priscillajoy@karunya.edu, [3]karuppasamyrvs@gmail.com

Orcid ID: [1]0000-0001-8469-1109, [2]0000-0001-5778-8415, [3]0000-0001-5309-6219

Abstract

The vulnerability of wireless networks to misclassification and security oversight is increased by adversarial attacks using Deep Learning (DL)-based Intrusion Detection Systems (IDS). Because they are unable to distinguish small fluctuations in signal data and retain spatial hierarchy, traditional neural networks prefer Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), which are highly prone to adversarial perturbations. In this research, a Capsule Network (CapsNet)-based framework detecting adversarial attacks in wireless networks is proposed. The network uses RF-aware capsule representations and dynamic routing to improve hierarchical feature learning and robustness against adversarial perturbations. To successfully search for adversarial distortion, the proposed model extracts significant network traffic features, encodes spatial hierarchy via primary and digit capsules, and uses a reconstruction loss function. To improve the model's robustness against sophisticated attack tactics, an exploratory quantum-assisted CapsNet implementation for preliminary investigation is also included. Experimental evaluation on benchmark wireless intrusion datasets shows that CapsNets outperform conventional CNNs and Long Short-Term Memory (LSTM) models, achieving 98.3% accuracy under normal conditions and maintaining 91.3% precision even under adversarial attack, compared to 87.5% and 72.4% for CNNs and 90.2% and 78.6% for LSTMs, respectively. In addition, compared with traditional DL models, CapsNets show a 34% improvement in robustness metrics. The proposed CapsNet system achieved 98.3% detection accuracy and a reduced False Positive Rate across several adversarial attack scenarios.

Keywords: Adversarial Attacks, Wireless Networks, Capsule Networks, Deep Learning, Dynamic Routing.

1. Introduction

The dynamic 5G/6G wireless environment is vulnerable to adversarial perturbations, which compromise the reliability of intruder detection. However, as their reliance on wireless networks increases, they have become a promising target for adversarial attacks [1]. The above attack exploits network weaknesses to interfere with support, steal confidential information, or

DOI: https://doi.org/10.36548/jtcsst.2026.3.008
Received: 06.05.2026, received in revised form: 11.06.2026, accepted: 30.06.2026, published: 10.07.2026

disrupt system performance. Although traditional safety measures such as authentication and encryption are often insufficient to prevent the complex, constantly evolving environment of adversarial attacks, they may still be somewhat effective [2]. Capsule Networks preserve part-whole relationships through vector capsules and routing-by-agreement mechanisms. Wireless signals contain hierarchical spatial and spectral dependencies represented by RSS, CSI and traffic statistics. Dynamic routing enables capsules to capture these relationships more effectively than scalar CNN representations, thereby improving robustness against perturbations and feature distortions generated by adversarial attacks.

To make wireless networks resilient to any kind of attack, studies are being conducted using different techniques, especially in ML, DL, and AI. Adversarial attacks on wireless networks can be of various types, which include jamming, spoofing, and eavesdropping. In a jamming attack, a highly intense signal is sent for the denial of service and blocking of legitimate communications. Recently, DL has proven itself to be quite effective in the detection and prevention of any type of malicious attack on wireless networks [3-7]. Such systems are ideal for detecting and preventing malicious actions in the wireless network environment.

1.1 Major Contributions of the Proposed Work

Innovation comes from the use of CapsNet technology to create a defense against adversarial attacks tailored to dynamic wireless networks. The approach differs from previous systems. While prior systems have concentrated mostly attack detection or on adversarial training, the new system incorporates routing-based hierarchical feature extraction, reconstruction loss-based anomaly detection, adaptive online learning, transfer learning, and resource optimization within the given architecture. In addition, the new system enables the detection of multiple types of attacks, such as evasion, poisoning, jamming, replay, and man-in-the-middle attacks, in the context of 5G/6G wireless networks.

The major contributions and technical advancements of the proposed work are as follows:

1. Detection of an adversarial attack framework using CapsNet for wireless networks that can handle multiple types of adversarial attacks through its architecture.
2. The incorporation of dynamic routing and reconstruction loss techniques for improved adversarial perturbation detection and hierarchical feature representation.
3. Integration of adaptive online and transfer learning techniques to improve the model's generalization in dynamic wireless network environments.
4. Resource optimization strategies, including pruning and quantification, to improve computational efficiency for real-time applications in resource-constrained environments.
5. The introduction of an adaptive RF-aware lightweight CapsNet system with optimized dynamic routing for effective adversarial mitigation in real-time wireless network architectures.
6. Preliminary investigation of hybrid Quantum Capsule Networks (QCapsNets) architectures as a potential future extension for improving feature representation and robustness in wireless IDS.

7. A wireless-specific mathematical formulation extending the original CapsNet through RF-aware feature representation, adaptive feature fusion, RF similarity-guided dynamic routing, adversarial confidence estimation, and joint optimization for robust wireless adversarial attack detection.

2. Literature Review

In contrast to conventional CNNs, Capsule Networks (CapsNets) employ a vector, or capsule, to record both the presence and the spatial connection of a feature, unlike the scalar end product familiar in feature representation [6-9]. However, CapsNet's use in wireless network security is still in its early stages [10-14]. CapsNets have been used to improve the reliability of spoof detection systems by more accurately mimicking the connection between genuine and fake signals [15]. Such a study demonstrates CapsNet's ability to withstand adversarial attacks in wireless networks [16–18]. Bandwidth and computing power are frequently limited in wireless networks [19]. Similarly, CapsNets require a batch of labeled data for training, which is difficult to obtain in the presence of an adversarial attack, as attack data are usually rare [20]. Standard assessments, which prioritize accuracy, may not be adequate for measuring CapsNet performance under adversarial attacks [21]. Rather, it is recommended to use metrics such as adversarial accuracy and robustness to assess the model's resistance to adversarial perturbations [22]. The approach frequently struggles to adapt to the dynamic, evolving nature of adversarial attacks that exploit system weaknesses to interfere with or steal confidential information [23]. DL-based approaches [24], notably CNNs [25] and RNNs [9] have shown that adversarial attacks can learn complex patterns in associated congestion and signal data [26, 27]. Despite their success, traditional DL models are vulnerable to adversarial input signals, particularly those crafted to deceive them, raising concerns about their reliability in adversarial environments [28]. CapsNets use vector-based capsules to represent features, allowing them to manage variations in input data, such as changes in position, scale, and perspective [30, 31]. Parasuraman et al. [27] present a system for detecting jamming attacks using CapsNet, which provides enhanced accuracy and robustness compared to CNNs. Likewise, CapsNet-based systems outperform CNN-based ones due to their enhanced representation of relationships between valid signals and spoofed ones.

However, several challenges still exist in applying CapsNets in wireless network security. First, the high computational complexity of CapsNet is a significant challenge, especially in wireless networks where bandwidth and resource are scarce. Consequently, given that attack data is scarce in the context of adversarial attacks, it will be difficult to obtain the large amount of labeled data needed for CapsNet training. Second, the interpretability of CapsNets depends on their dynamic routing process and vector-based representation, which makes it difficult to investigate and understand how the model reaches its decisions. Generative Adversarial Networks (GANs) have been studied as a defensive mechanism for adversarial training, enhancing the model's robustness against attack variations, but these models frequently suffer from training instability and mode collapse, making them unreliable for wireless security applications [33]. Moreover, adversarial attacks, such as graph perturbation attacks, can compromise Graph Neural Network (GNN)-based IDS models by modifying system configurations to evade detection [34]. Transformer-based models, such as BERT and Vision Transformers (ViTs) can capture long-range dependencies and are promising for wireless applications.

Existing CNN-, RNN-, GAN-, and Transformer-based IDS models mainly optimize classification accuracy but seldom investigate robustness against adversarial perturbations. Most studies focus on single attack categories and not explicitly model attack generation parameters. Moreover, existing architectures fail to preserve hierarchical RF feature relationships inherent in wireless communication signals. Therefore, there is a need for a robust feature representation framework capable of maintaining structural dependencies while improving adversarial resilience.

3. Proposed System

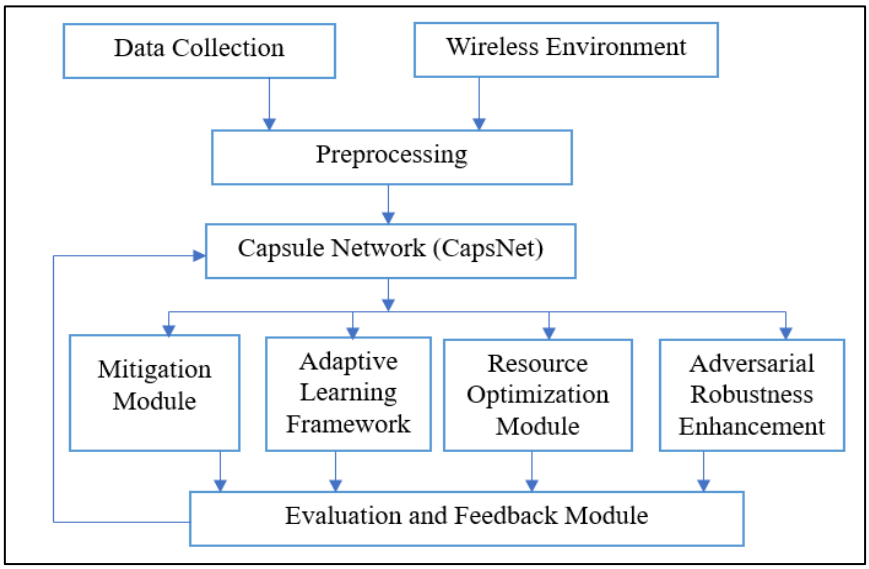

Figure 1. Proposed RF-aware capsule network architecture for adversarial attack detection in wireless networks

A secure, adaptable security framework using Capsule Networks (CapsNet) is proposed to solve the problem of defending against adversarial attacks in wireless networks. From the figure below, the framework for detecting adversarial attacks in wireless networks using CapsNet includes many components that detect, analyse, and defend against adversarial attacks. Development of the adaptive RF-aware CapsNet framework for detecting adversarial attacks in wireless networks is the core technical contribution of the proposed framework. Unlike standard CapsNet-based intrusion detection approaches, the proposed method introduces RF-aware capsule attribute encoding to maintain the hierarchical spatial and spectral interfaces inherent in wireless communication signals. Moreover, an adaptive adversarial defense mechanism is integrated to dynamically improve robustness against increasing attack perturbations.

3.1 Data Collection

The experiment used a 6G wireless channel estimation and adversarial attack dataset derived from a simulated 5G/6G wireless communication environment. As shown in Table 1, the dataset was generated using NS-3 and MATLAB 5G Toolbox simulations. Normal traffic samples consisted of legitimate wireless transmissions. Adversarial samples were generated by injecting perturbations corresponding to evasion, replay, jamming and man-in-the-middle attacks.

Table 1. Dataset characteristics and input feature configuration [35-36]

Parameter	Value

Total Samples	52,000
Normal Samples	26,000
Adversarial Samples	26,000
Number of Classes	6
Attack Categories	Evasion, Poisoning, Replay, Jamming, MITM
Feature Dimension	128 × 1
Feature Types	RSS, SNR, CSI, Latency, Packet Statistics
Dataset Environment	Simulated 5G/6G Wireless Network
Simulation Tools	NS-3 + MATLAB 5G Toolbox
Data Preprocessing	Min-Max Normalization

3.1.1 Adversarial Attack Modeling

To evaluate the robustness of the proposed CapsNet framework, adversarial samples were generated using FGSM, PGD, BIM, CW, and DeepFool algorithms. The attacks were applied to normalized wireless feature vectors consisting of RSS, SNR, CSI, packet statistics, latency, and flow descriptors. For FGSM and BIM attacks, perturbation budgets $\varepsilon = 0.01, 0.03$, and 0.05 were used. PGD was implemented with 20 iterations and a step size $\alpha=0.005$. DeepFool employed 50 maximum iterations, whereas the CW attack used confidence parameter $\kappa=0$ and a learning rate of 0.001. Poisoning attacks were simulated during the training phase by randomly corrupting class labels. Label corruption ratios of 5%, 10%, and 15% were considered. The objective was to evaluate model degradation caused by manipulated training data rather than perturbations during inference. The attack success rate and adversarial accuracy were used to quantify robustness.

3.2 Preprocessing

The extracted input feature vector consists of RF signal features (RSS, SNR, CSI), network traffic statistics (packet rate, packet loss, rotational latency), and modulation-related parameters, which were normalized using Min-Max normalization prior to being fed into the CapsNet architecture.

3.3 Attack Detection

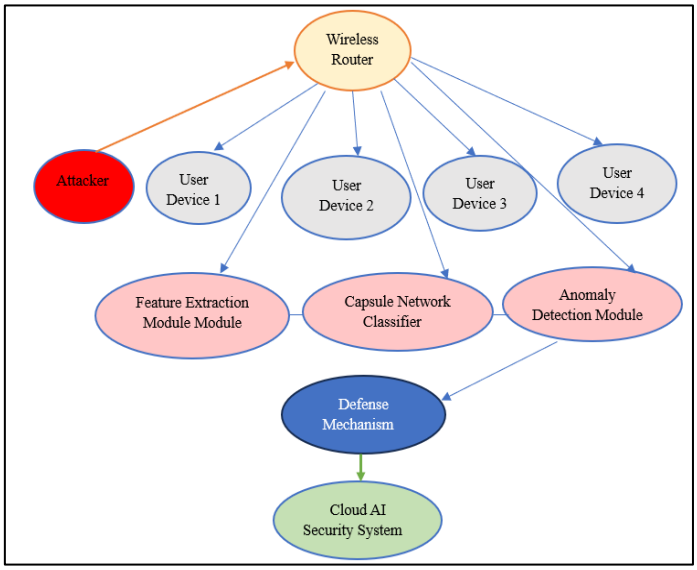

Figure 2. RF-aware capsule network-based adversarial attack detection framework

Figure 2 shows a DL-based model for mitigating adversarial attacks in wireless networks using capsule connections. The wireless router, which connects several user devices

to the network, is located near the central part. An attacker node attempts to inject adversarial traffic into the system by exploiting a vulnerability. The feature extraction module collects router information and identifies the most important network congestion structure. The CapsNet classifier, which uses an active path to identify adversarial manipulation more effectively than a typical DL model, then feeds the compiled features into the classifier. Further anomaly-detection modules monitor deviations in associated activities and warn of potential vulnerabilities. Thus, the defense mechanism reduces the attack surface and provides forward protection of the Cloud AI security system, continuously enhancing its real-time safety. This approach guarantees the existence of wireless networks that can protect themselves against increasing threats. The above-described architecture is applicable not only to wireless networks like IoT and 5G but also to future frameworks.

3.4 Future Mitigation Extensions

After an attack is detected, other forms of mitigation such as rerouting traffic, isolation of compromised devices, and frequency hopping can be implemented in the future. These mechanisms were not implemented in the current study.

3.5 Adaptation and Learning

The adaptation and learning phase ensure the framework's longevity by continuously updating the model through online learning and transfer learning techniques. This enhances it's ability to distinguish and respond to evolving malicious threats in real time by enabling it to adapt to new attack patterns and adjust its network configuration.

3.6 Evaluation and Feedback

A robustness approach similar to adversarial precision and FPR is used during the evaluation and feedback phase to assess the system's performance. The model's ability to detect and counter adversarial attacks in wireless networks can be improved by leveraging information from the assessment.

3.7 Components of the Proposed System

The proposed approach consists of several essential components that aim to enhance the detection of adversarial attacks in wireless networks using a Capsule Network-based methodology. It has a powerful detection engine that models aspect association and uses dynamic routing to detect slight suspicious perturbations. Adversarial training and data augmentation techniques are applied to increase resistance to adversarial attacks and ensure effective detection even in the presence of existing fraudulent threats. In addition, the compression methods improve computational efficiency, enabling the model to be used in wireless environments with limited resources.

3.7.1 Capsule Network-Based Detection Engine

The Capsule Network-based Detection Engine uses a CapsNet architecture to process wireless system statistics, including robustness, traffic pattern, and spectral features, to detect adversarial networks. By using dynamic routing, CapsNets model feature associations,

allowing them to detect subtle adversarial perturbations that conventional CNNs would overlook.

3.7.2 Adversarial Robustness Enhancement

Using adversarial cases during training, adversarial training enhances CapsNet's capacity and ensures its structure is impervious to attack. Data augmentation is used to further enhance detection capacity by creating synthetic adversarial scenarios, handling limited labeled attack data, and improving the model's generalization across different adversarial contexts.

3.7.3 Resource Optimization

Pruning, quantization, and understanding distillation are among the model compaction techniques used to reduce CapsNet's computational complexity, thereby enabling it to function efficiently in a wireless scenariowith limited resources. Moreover, the edge deployment architecture requires processing neighborhood statistics to reduce latency and improve the ability of wireless networks to detect malicious threats in real time.

3.7.4 Adaptive Learning Framework

Transfer learning can be used with a pre-trained CapsNet model in a specific wireless network environment, thereby reducing reliance on extensive label statistics and speeding up model adaptation. The system also integrates online learning capabilities, which enhance its ability to recognize recent adversarial threats by enabling it to continuously adapt to evolving attack forms and active system environments for a longer period.

3.7.5 Comprehensive Evaluation Framework

It is intended to evaluate the capability and performance of the Capsule Network-based detection structure against malicious attempts on wireless networks. To quantify the system's robustness, the assessment procedure integrates several robustness metrics, including adversarial accuracy, robustness score, and FPR. Moreover, the system checks the model under different adversarial attack scenarios. The framework will undergo simulations in a dynamic wireless environment to test its ability to locate a hazard while maintaining minimal rotational motion and to confirm its versatility.

3.7.6 Exploratory Quantum-Assisted CapsNet Implementation

In addition to the classical CapsNet architecture, an exploratory hybrid Quantum-Assisted CapsNet (QCapsNet) framework was investigated to examine the feasibility of integrating variational quantum circuits with capsule-based feature learning. The purpose of this extension is to explore the potential of quantum-assisted feature representations rather than to establish a new state-of-the-art architecture for adversarial attack detection in wireless networks. The quantum module employs a four-qubit variational circuit implemented using the Qiskit Aer simulator. The number of qubits was selected to maintain computational feasibility and demonstrate proof-of-concept integration with the capsule network architecture. Since the experiments were conducted entirely in a simulated environment, no implementation on physical quantum hardware was performed. Quantum circuits proceed through an angle embedding layer, followed by parameterized rotational gates and entanglement operations. The quantum state of transformation is represented as shown in equation (1).

$$| \psi\rangle = U(\theta)H^{\otimes n} | 0\rangle^{\otimes n} \quad (1)$$

where $U(\theta)$represents the trainable parameterized quantum circuit and H denotes the Hadamard transformation applied to initialize quantum superposition states.

Table 2. Quantum-assisted CapsNet configuration

Parameter	Value
Quantum Framework	PennyLane + Qiskit
Quantum Simulator	Qiskit Aer Simulator
Number of Qubits	4
Variational Layers	3
Quantum Embedding	Angle Embedding
Entanglement Type	CNOT
Quantum-Classical Model	Hybrid QCapsNet

The experiment was conducted using the IBM Qiskit Aer Simulator with 4 qubits and 3 quantum layers. The model was trained using the Adam optimizer with a learning rate of 0.001, a batch size of 32, and 50 epochs. To ensure consistency and enable fair comparison, the same wireless adversarial attack dataset employed in the classical CapsNet experiment was used. In the hybrid Quantum-Assisted CapsNet framework, the classical training configuration remained unchanged, whereas the additional quantum simulation parameters are reported separately in Table 2. Preliminary simulation results indicated a modest improvement in classification performance compared with the classical CapsNet model. This quantum-enhanced method is for the purposes of proof-of-concept. The application of the four-qubit variational circuit and simulator model limits the generalizability of the findings. There is a need for further research to be conducted using more complex quantum circuits, quantum computing hardware, and full benchmarks to make conclusions about the practical benefits of QCapsNet.

3.8 Mathematical Model for Implementation

Different from the traditional Capsule Network, which was initially designed for image recognition, the mathematical formulation introduced in this research has been modified to accommodate the requirements of detecting RF-aware adversarial attacks in wireless communications. The mathematical innovations included in the introduced mathematical formulation are the incorporation of wireless signal features, RF feature fusion, feature weight by attention, RF similarity-based dynamic routing, adversarial confidence calculation, and joint optimization for robust wireless intrusion detection.

3.8.1 RF-Aware Feature Representation

Wireless communication networks generate heterogeneous physical-layer and network-layer measurements that reflect the operational state of the network. Unlike conventional Capsule Networks, which process image pixels, the proposed framework utilizes RF-aware communication features for adversarial attack detection. Each wireless communication sample is represented as a multidimensional feature vector composed of signal quality indicators and network traffic characteristics. The input feature vector is defined as shown in equation (2).

$$\mathrm{x}_i = \begin{bmatrix} RSS_i \\ SNR_i \\ CSI_i \\ L_i \\ P_i \end{bmatrix} \quad (2)$$

where:

- x_i denotes the RF-aware feature vector corresponding to the i^{th}wireless communication sample.
- RSS_i represents the Received Signal Strength, which indicates the received power level of the wireless signal.
- SNR_i denotes the Signal-to-Noise Ratio, representing the quality of signal reception.
- CSI_i represents the Channel State Information describing channel propagation characteristics.
- L_i denotes the communication latency measured during packet transmission.
- P_i represents packet-level statistical information such as packet loss rate, packet arrival interval, retransmission count, and throughput.

In contrast to conventional CapsNet that directly processes image pixels, the proposed model represents each communication instance using heterogeneous RF descriptors extracted from the wireless physical and network layers. This representation enables the capsule network to preserve wireless-specific characteristics required for adversarial attack detection.

3.8.2 RF Feature Normalization

Given that the wireless attributes obtained have different physical units and ranges,this can bias the learning towards those wireless attributes having bigger values. In order to allow each wireless attribute to contribute equally during learning, Min-Max Normalization is used. The formula for normalizing wireless attributes is illustrated in equation (3).

$$\hat{x}_{ij} = \frac{x_{ij} - x_j^{\min}}{x_j^{\max} - x_j^{\min}} \quad (3)$$

where:

- x_{ij} denotes the original value of the j^{th}feature in the i^{th}sample.
- $\hat{x}_{ij}$ represents the normalized feature value.
- $x_j^{\min}$ denotes the minimum observed value of feature j.
- $x_j^{\max}$ denotes the maximum observed value of feature j.

All the features have been scaled within the range of [0,1] through this normalization, which ensures the stability of the numerical algorithm and avoids any dominance of wireless features due to their magnitude.

3.8.3 RF Feature Fusion

After normalization, the individual RF features are fused to derive a combined representation of the wireless signal's communication attributes. The equal importance of all features has not been considered; rather, a trainable weight mechanism has been introduced to make the learning process adaptive. The fused representation of the feature can be derived using equation (4).

$$F_i = W_r RSS_i + W_s SNR_i + W_c CSI_i + W_l L_i + W_p P_i + b \quad (4)$$

where:

- F_i denotes the fused RF feature representation.
- W_r is the learnable weight corresponding to Received Signal Strength.
- W_s is the learnable weight corresponding to Signal-to-Noise Ratio.
- W_c denotes the weight associated with Channel State Information.
- W_l represents the weight assigned to latency.
- W_p denotes the weight corresponding to packet statistics.
- b is the bias parameter.

The adaptive feature fusion method is not present in the original CapsNet model. It helps in assigning automatic weights to the RF data based on its usefulness under different types of wireless attacks.

3.8.4 RF Feature Attention

Wireless features have different significance levels for each type of attack. For that reason, an attention method has been introduced to assign dynamic weights to the fused feature vector. The attention factor can be calculated using the Softmax function, as stated below.

$$\alpha_i = \frac{\exp(F_i)}{\sum_{k=1}^{N} \exp(F_k)} \quad (5)$$

where:

- α_i denotes the attention weight assigned to the i^{th} feature representation.
- F_i is the fused RF feature score.
- N denotes the total number of feature vectors.

The Softmax operation converts feature scores into normalized probabilities whose sum equals one. Consequently, features carrying more discriminative information receive larger attention weights, while less informative features are suppressed. This adaptive weighting improves the robustness of feature learning under different adversarial attack conditions. Unlike conventional CapsNet, the proposed attention mechanism selectively amplifies RF features that exhibit higher discriminative capability for wireless adversarial attack detection.

3.8.5 Capsule Feature Encoding

The weighted RF features are encoded into capsule vectors prior to higher-level representation learning. The capsule input is defined as shown in equation (6).

$$u_i = \alpha_i F_i \tag{6}$$

where:

- u_i denotes the capsule input vector.
- α_i represents the attention coefficient.
- F_i denotes the fused RF feature representation.

This operation amplifies informative wireless characteristics while reducing the influence of noisy or redundant features. Consequently, the capsule layer receives a compact yet discriminative representation of the wireless communication environment.

3.8.6 RF-Aware Capsule Transformation

Each capsule input vector is transformed into a higher-level feature space through a trainable transformation matrix. The prediction vector is obtained as shown in equation (7).

$$\hat{u}_{j|i} = W_{ij}^{RF} u_i \tag{7}$$

where:

- $\hat{u}_{j|i}$ denotes the prediction vector generated by capsule $i$for higher-level capsule j.
- W_{ij}^{RF} represents the RF-aware transformation matrix.
- u_i denotes the capsule input vector.

The transformation matrix learns complex relationships among wireless communication features and projects low-level RF representations into higher-level semantic representations suitable for attack identification.

3.8.7 RF Similarity-Guided Dynamic Routing

Dynamic routing establishes communication between lower-level and higher-level capsules based on feature agreement. In the proposed framework, routing additionally incorporates RF similarity to strengthen feature consistency. The routing coefficient is calculated as shown in equation (8).

$$c_{ij} = \frac{\exp\left(b_{ij} + \gamma S_{ij}\right)}{\sum_k \exp\left(b_{ik} + \gamma S_{ik}\right)} \tag{8}$$

where:

- c_{ij} denotes the routing coefficient.
- b_{ij} is the routing logit.

- γ is the RF similarity weighting parameter.
- S_{ij} denotes the cosine similarity between capsule vectors.

The RF similarity is computed as shown in equation (9).

$$S_{ij} = \frac{u_i^T v_j}{\|u_i\| \|v_j\|} \tag{9}$$

where:

- u_i represents the lower-level capsule vector.
- v_j denotes the higher-level capsule vector.
- $\|\cdot\|$ represents the Euclidean norm.

The original CapsNet performs routing exclusively based on agreement between prediction vectors. The proposed routing algorithm additionally incorporates RF similarity computed from wireless communication features. Consequently, capsules exhibiting similar RF behavior receive higher routing coefficients, allowing the model to preserve hierarchical wireless feature relationships and improve robustness against adversarial perturbations.

3.8.8 Adversarial Attack Detection

The final capsule output is computed using the routing coefficients.

$$v_j = Squash\left(\sum_i c_{ij}\, \hat{u}_{j|i}\right) \tag{10}$$

where:

- v_j denotes the output vector of capsule j.
- c_{ij} is the routing coefficient.
- $\hat{u}_{j|i}$ is the prediction vector.

The squash activation ensures that capsule vector lengths remain within the interval [0,1], where larger vector lengths correspond to higher confidence. The adversarial confidence score is calculated as shown in equation (11).

$$A_i = \max_j \| v_j \| \tag{11}$$

where:

- A_i denotes the confidence score for the detected attack.
- $\| v_j \|$ denotes the Euclidean norm of capsule j.

The adversarial confidence score represents a wireless-specific decision criterion introduced in this work. Unlike the original CapsNet, which uses capsule length solely for class prediction, the proposed framework interprets capsule confidence as an adversarial attack score

that is subsequently compared with a detection threshold. The attack decision is then obtained using equation (12).

$$D_i = \begin{cases} Attack, & A_i > \tau \\ Normal, & A_i \leq \tau \end{cases} \tag{12}$$

where:

- D_i denotes the final detection result.
- τ represents the predefined detection threshold.

If the confidence score exceeds the threshold, the sample is classified as an adversarial attack; otherwise, it is considered legitimate wireless communication. The proposed attack detection mechanism consists of two sequential stages. First, RF similarity-guided dynamic routing generates discriminative capsule representations by aggregating hierarchical wireless communication features. Second, the length of the output capsule is interpreted as an adversarial confidence score and compared with a predefined detection threshold to classify the sample as legitimate or adversarial. Therefore, dynamic routing contributes indirectly by improving feature representation, while the confidence-based decision module performs explicit attack detection.

3.8.9 Model Optimization

The network is optimized by jointly minimizing the classification loss and adversarial detection loss.

$$L = L_{cls} + \lambda L_{adv} \tag{13}$$

where:

- L denotes the total optimization loss.
- L_{cls} is the classification loss.
- L_{adv} represents the adversarial detection loss.
- λ controls the contribution of the adversarial detection objective.

The proposed optimization objective extends the conventional CapsNet loss by jointly minimizing classification loss and adversarial detection loss, thereby improving robustness under adversarial wireless communication scenarios. The adversarial detection loss is computed as shown in equation (14).

$$L_{adv} = -\frac{1}{N}\sum_{i=1}^{N} y_i \log(\hat{y}_i) \tag{14}$$

where:

- N is the number of training samples.
- y_i denotes the ground-truth label.
- $\hat{y}_i$ represents the predicted probability.

The combined objective function simultaneously improves classification accuracy and enhances the robustness of the proposed framework against adversarial attacks in wireless communication networks.

3.9 Algorithm of Proposed RF-Aware Capsule Network for Adversarial Attack Detection and Mitigation

Input: Wireless Packet Stream: $P = \{P_i\}_{i=1}^{N}$
Initialization:

- Initialize network parameters: $\Theta = \{W, b\}$
- Initialize routing iterations: r
- Initialize learning rate: η
- Initialize detection threshold: τ
- Initialize security event log: $L \leftarrow \emptyset$

Step 1: RF Feature Extraction
Extract RF-aware feature vector: $x_i = \left[RSS_i,\ SNR_i,\ CSI_i,\ R_{p,i},\ L_i,\ PLR_i,\ M_i,\ T_{f,i}\right]^T \in \mathbb{R}^d$
Step 2: Feature Normalization
Normalize every feature using Min-Max normalization: $\bar{x}_i = \frac{x_i - x_{min}}{x_{max} - x_{min}}$
Step 3: RF Feature Fusion
Generate fused feature representation: $F_i = W_f \bar{x}_i + b_f$, where: $W_f \in \mathbb{R}^{m \times d}$
Step 4: RF Attention Computation
Compute attention weights: $\alpha_i = \frac{\exp(F_i)}{\sum_{k=1}^{N} \exp(F_k)}$
Step 5: Capsule Feature Encoding
Generate capsule input vectors: $u_i = \alpha_i \odot F_i$
Step 6: RF-Aware Capsule Transformation
Transform the capsule vectors: $\hat{u}_{j|i} = W_{ij}^{RF} u_i$
Step 7: Initialize Routing
Initialize routing logits: $b_{ij} = 0$
Step 8: RF Similarity-Guided Feature Aggregation using Dynamic Routing
For $t = 1, 2, \ldots, r$
Compute:

Routing coefficients: $c_{ij} = \frac{\exp(b_{ij} + \gamma S_{ij})}{\sum_k \exp(b_{ik} + \gamma S_{ik})}$

RF similarity: $S_{ij} = \frac{u_i^T v_j}{\|u_i\|_2 \|v_j\|_2}$

Capsule input: $s_j = \sum_i c_{ij} \hat{u}_{j|i}$

Capsule output: $v_j = \text{squash}(s_j)$

Update routing logits: $b_{ij} \leftarrow b_{ij} + \hat{u}_{j|i}^T v_j$

Repeat for r routing iterations.
Step 9: Compute Capsule Confidence Score
Compute: $A_i = \max_j \left(\| v_j \|_2\right)$
Step 10: Threshold-Based Adversarial Attack Detection
If $A_i > \tau$ then

$\hat{y}_i = \arg\max_j \| v_j \|_2$

Else $\hat{y}_i = \text{Normal}$
Step 11: Attack Mitigation
If $\hat{y}_i = \text{Normal}$ then

$a_i = \text{Allow\_Transmission}()$

Else

$a_i = \text{Mitigation}(\hat{y}_i)$

Record the security event: $L \leftarrow L \cup \{P_i, \hat{y}_i, a_i, t\}$

Generate administrator alert.

Step 12: Model Optimization

Compute overall loss: $L = L_{cls} + \lambda L_{adv}$

Update network parameters using learning rate: η

End

Output:

- Predicted attack class: $\hat{y}_i \in Y$
- Mitigation action: a_i

4. Results and Discussions

To evaluate the effectiveness of the proposed Capsule Network defense mechanism, it is necessary to measure the performance of adversarial attack detection in wireless networks. By reducing misclassification, this approach enhances the system's ability to distinguish and classify adversary attacks.

4.1 Experimental Setup

The proposed CapsNet-based adversarial attack detection system was implemented using Python, TensorFlow, and PyTorch. The experiment was performed on a computer equipped with an Intel Core i9 processor, NVIDIA RTX 4090 GPU, 24 GB of RAM, and an Ubuntu 22.04 operating system. To improve training effectiveness, CUDA acceleration is necessary. The experimental evaluation was conducted using the dataset described in Section 3.1. Table 3 presents the hyperparameter settings used to train the CapsNet model for adversarial attack detection in wireless networks. To identify overfitting and improve generalization, a dropout rate of 0.3 was used. The dynamic routing mechanism uses three iterations to provide a robust feature representation within the capsule layer.

Table 3. Hyperparameter settings used for CapsNet training

Parameter	Value
Optimizer	Adam
Learning Rate	0.001
Batch Size	64
Epochs	100
Dropout Rate	0.3
Routing Iterations	3
Training Split	70%
Validation Split	15%
Testing Split	15%
Poisoning Ratio	5%,10%,15%
Label Corruption	Random
Corrupted Samples	Training set only

4.2 Performance Analysis

Table 4 presents the correlation between the performance of the CapsNet model and conventional CNN and RNN approaches for adversarial attack detection in wireless networks. The CapsNet model achieved 98.3% accuracy, exceeding CNN and RNN models. It also shows

high accuracy (97.8%), recall (98.2%), and F1-score (98.2%), demonstrating its ability to accurately identify adversarial attacks and minimize classification error. In addition, CapsNet had the lowest computational time of 32.4 ms, compared to CNN (41.2 ms) and RNN (45.6 ms), demonstrating its suitability for real-time wireless security functions.

Table 4. Performance comparison

Metric	CapsNet Model	CNN-Based Model [25]	RNN-Based Model [9]
Accuracy (%)	98.3	94.5	92.8
Precision (%)	97.8	92.6	91.3
Recall (%)	98.2	95.7	93.9
F1-Score (%)	98.0	94.1	92.6
False Positive Rate (FPR)	0.024	0.056	0.072
False Negative Rate (FNR)	0.018	0.043	0.061
Detection Rate (%)	97.9	93.8	91.7
AUC	0.99	0.93	0.89
Computational Time (ms)	32.4	41.2	45.6

Table 5. Experimental comparison of classical CapsNet and quantum-assisted CapsNet

Metric	CapsNet	QCapsNet
Accuracy (%)	98.3	98.9
Precision (%)	97.8	98.5
Recall (%)	98.2	98.7
F1-Score (%)	98.0	98.6
FPR	0.024	0.017
FNR	0.018	0.013
Detection Rate (%)	97.9	98.8
Inference Time (ms)	32.4	35.1

As shown in Table 5, the experimental evaluation of the Quantum-Assisted Capsule Network (QCapsNet) shows improved performance compared to the classical CapsNet. QCapsNet achieves a 98.9% accuracy rate, surpassing the classical CapsNet's accuracy of 98.3%. The model also improves the capability to detect adversarial attacks by reducing the FPR from 0.024 to 0.017 and the FNR from 0.018 to 0.013. Moreover, the detection rate was increased to 98.8%, demonstrating improved robustness against a wireless network attack.

Table 6. Performance before and after adversarial attacks

Metric	Clean Data	Under Adversarial Attack
Accuracy (%)	98.3	91.3
Precision (%)	97.8	91.3
Recall (%)	98.2	90.7
F1-score (%)	98.0	91.0
FPR	0.024	0.083
Detection Rate (%)	97.9	91.2

Table 6 compares the performance of the proposed CapsNet under clean and adversarial conditions. Under clean traffic, the model achieved an accuracy of 98.3%. When evaluated using adversarial examples generated by FGSM, PGD, BIM, DeepFool, and CW attacks, the accuracy decreased to 91.3%, while maintaining high robustness compared with conventional CNN and RNN models. These results demonstrate that the proposed RF-aware CapsNet preserves strong detection capability even in the presence of adversarial perturbations.

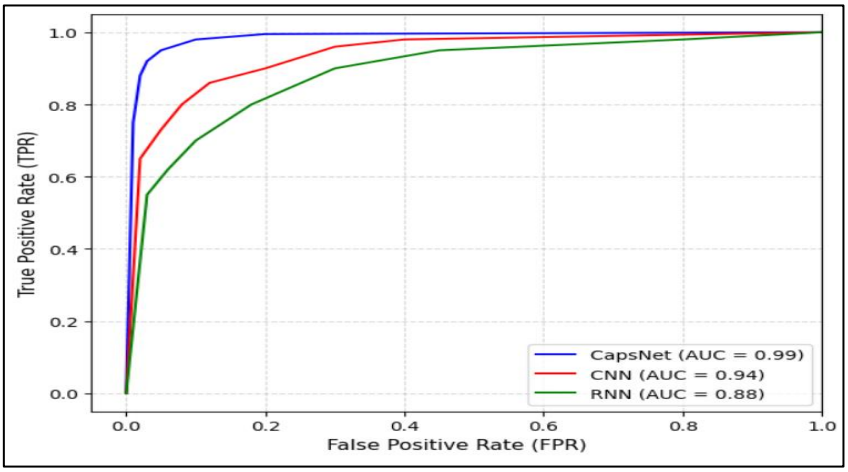

Figure 3. ROC curve comparison for adversarial attack detection in wireless networks using CapsNet, CNN [25], and RNN [9]

For the CapsNet, CNN, and RNN models, the ROC curves in Figure 3 show the trade-off between the TPR and the FPR. The proposed CapsNet achieved a high AUC of 0.99, demonstrating excellent discriminative ability for adversarial attack detection. Furthermore, the ROC evaluation remains unchanged, along with the quantitative results reported in Table 5, where CapsNet achieved an FPR of 0.024, compared to CNN (FPR = 0.056) and RNN (FPR = 0.072). The low FPR indicates that the proposed system adequately minimizes false alarms while maintaining higher detection efficiency. The robustness of CapsNet against adversarial and malicious network congestion is substantiated by the higher AUC and lower FPR.

4.2.1 Adversarial Attack Configuration

The adversarial attack configurations described in Section 3.1.1 were used for experimental evaluation, and the corresponding attack success rates are presented in Table 7. These settings provide a reproducible experimental configuration for evaluating adversarial robustness.

Table 7. Experimental settings and attack success rates for FGSM, BIM, PGD, DeepFool, and CW attacks

Attack Method	Perturbation Budget (ε)	Iterations	Step Size (α)	Attack Success Rate (%)
FGSM	0.01, 0.03, 0.05	1	-	86.4
BIM	0.03	10	0.005	82.1
PGD	0.03	20	0.005	79.8
DeepFool	-	50	Adaptive	76.3
CW	κ=0	100	Learning rate=0.001	74.9

Figure 4 represents the number of correctly detected adversarial samples for five different types of attacks:FGSM, PGD, DeepFool, CW, and BIM. In each case, 500 adversarial samples were created according to the parameters in Table 7. This comparison reflects the robustness of the CapsNet compared to CNN and RNN baselines against standard adversarial attacks.

According to Table 8, CapsNet effectively resists adversarial attacks, with enhanced detection efficiency and reduced FPR. Evasion (91.8%) and jamming (94.3%) are the most robust adversarial attacks; mitigation performance metrics reflect the capability of detecting

potential risks. Adversarial training also enhances the robustness of the model by decreasing the probability of success of adversarial attacks.

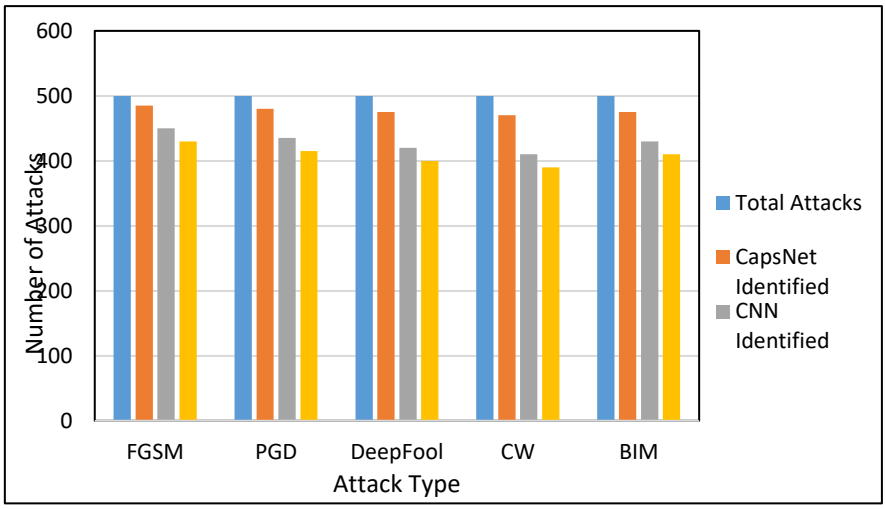

Figure 4. Comparison of adversarial attacks and identified cases by CapsNet, CNN [25], and RNN [9]

Table 8. Performance Evaluation of Adversarial Attack Detection in Wireless Networks Using Capsule Networks

Attack Type	Detection Accuracy (%)	False Positive Rate (FPR) (%)	Mitigation Effectiveness (%)
Evasion Attack	94.5	5.2	91.8
Poisoning Attack	92.3	6.5	89.7
Jamming Attack	96.1	3.8	94.3
Replay Attack	95.4	4.1	92.5
Man-in-the-Middle (MITM)	93.8	5.7	90.6

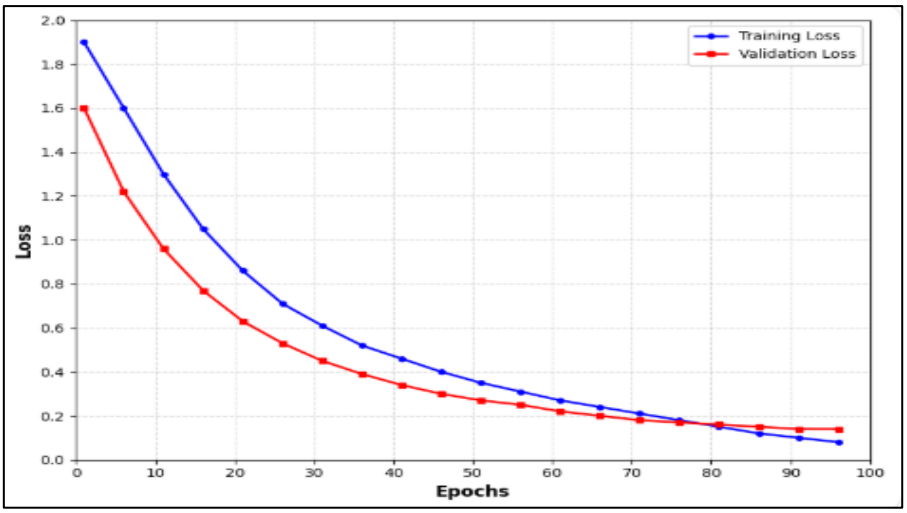

Figure 5. Training loss vs. epochs

Figure 5 summarizes the variation in training and validation loss over the CapsNet model. The graphs show a steady decrease in both the training and validation loss as the number of epochs increases, indicating stable training and efficient parameter optimization. The curve converges after the 75th epoch, demonstrating that the model achieves stable training without significant overfitting.

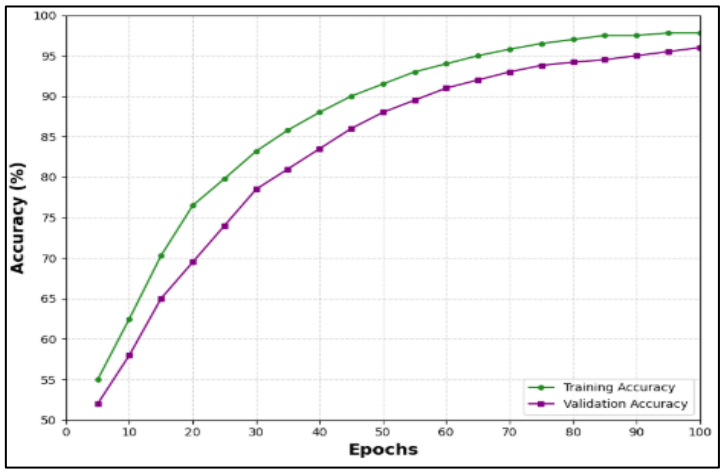

Figure 6. Validation accuracy vs. epochs

Figure 6 shows the accuracy of the CapsNet model during training and validation over several epochs. Precision continuously improves over epochs, reaching convergence at the 75th epoch and achieving a validation accuracy of 95%.

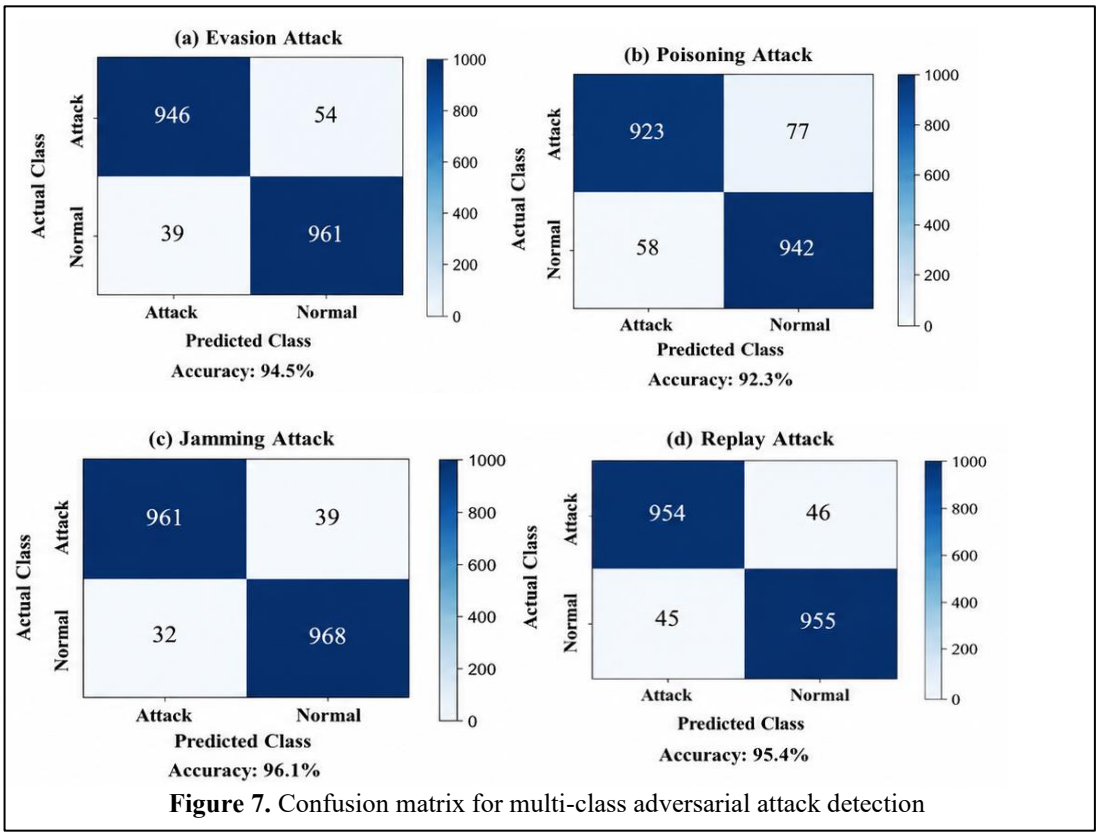

Figure 7. Confusion matrix for multi-class adversarial attack detection

For Evasion, Poisoning, Jamming, Replay, and MITM attacks, Figure 7 provides a specific confusion matrix. The CapsNet model achieves high categorization performance by combining all attack groupings with Jamming and Replay attacks for high detection accuracy. The reduced FNR and FPR demonstrate the robustness of the proposed framework in accurately characterizing adversarial attacks from normal network traffic.

4.2.2 Statistical Validation

To determine whether the observed improvements are statistically significant, paired t-tests were performed between the proposed CapsNet and the baseline CNN and RNN models using the results obtained from five repeated trials. As shown in Table 9, the resulting p-values were below 0.05, indicating that the performance improvements achieved by the proposed framework are statistically significant at the 95% confidence level.

Table 9. Statistical significance analysis using paired t-Test

Comparison	t-value	p-value
CapsNet vs CNN	8.72	<0.05
CapsNet vs RNN	10.35	<0.05

4.2.3 Ablation Study Analysis

The results of the ablation study indicate that all components of the CapsNet architecture are important for adversarial attack prevention, as shown in Table 10Disabling iterative routing reduced the average classification accuracy from 98.3% to 93.6%, demonstrating that dynamic routing contributes to improved feature representation and enhanced robustness under adversarial perturbations. Therefore, the role of dynamic routing should be interpreted as strengthening representation learning and robustness rather than serving as an explicit attack detection mechanism. Removing adversarial training and reconstruction loss resulted in noticeable performance degradation. The relatively small standard deviations observed across repeated trials indicate that the ablation results are stable and reproducible.

Table 10. Ablation study of proposed CapsNet framework

Model Configuration	Accuracy (%)	Mean ± SD
Full CapsNet Framework	98.3	98.3 ± 0.42
Without Dynamic Routing	93.6	93.6 ± 0.58
Without Adversarial Training	92.8	92.8 ± 0.63
Without Reconstruction Loss	94.1	94.1 ± 0.54
Without Adaptive Learning	95.2	95.2 ± 0.49

4.2.4 k-Fold Cross Validation

Table 11. 5-Fold cross-validation results of the proposed CapsNet framework

Fold	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Fold 1	98.0	97.5	96.4	96.9
Fold 2	98.2	97.7	96.8	97.2
Fold 3	98.4	98.0	97.1	97.5
Fold 4	97.9	97.3	96.2	96.7
Fold 5	98.1	97.6	96.6	97.0
Average	98.1	97.6	96.6	97.1

As shown in Table 11, the data were partitioned into five identical subsets, where four subsets were used for training and one subset for testing at each iteration. The average precision achieved across all folds was 98.1%, demonstrating the robustness and uniformity of the CapsNet under different data distributions.

4.2.5 Real-Time Deployment Considerations

The real-time deployment of the proposed lightweight CapsNet structure in 5G/6G wireless environments requires simplified edge processing, low inference latency, energy efficiency, and support for IoT resource constraints. The intended model reduces the parameter count to 6.2M, memory usage to 645 MB, and inference runtime latency to 32.4 ms by restricting the iteration rate to 3 and integrating pruning and quantization. The framework also achieved 194 watts of energy consumption and processed 5280 packets per second, which is suitable for 5G base stations and IoT gateways. Moreover, the lightweight architecture has improved its ability to exploit resources in dynamic wireless flow situations, ensuring 98.3% detection accuracy and reducing the FPR.

5. Conclusion

This research introduces a robust adversarial attack detection framework for wireless networks using Capsule Networks (CapsNets), addressing a fundamental vulnerability in DL-based intrusion detection structures. The CapsNet-based method, intended to be used against evasion, poisoning, jamming, and replay attacks, has been well adapted to resist them by exploiting active routing, hierarchical feature encoding, and a reconstruction loss function. The experimental results show that CapsNets outperform CNNs and LSTMs in terms of both detection accuracy and robustness, even under adversarial attack conditions. In addition, the proposed model optimizes resource allocation and enhances the adaptability of wireless network security through transfer learning and an online learning mechanism. Future research will focus on optimizing computational efficiency, investigating hybrid models combining CapsNets with Reinforcement Learning (RL) methods, and evaluating performance in large-scale infrastructure environments.

References

[1] Adesina, Damilola, Chung-Chu Hsieh, Yalin E. Sagduyu, and Lijun Qian. "Adversarial Machine Learning in Wireless Communications Using RF Data: A Review." IEEE Communications Surveys & Tutorials 25, no. 1 (2022): 77-100.

[2] Mehta, Shiva, Vinay Kukreja, Ayush Dogra, and Tejinder Pal Singh Brar. "Hybrid ViT-CapsNet Framework for Brain Tumor Diagnosis Using Biomedical MRI." Biomedical and Pharmacology Journal 18, no. March Spl Edition (2025): 99-119.

[3] Muthusamy, Rajendiran, Charulatha Kannan, Jayarathna Mani, Rathinasabapathi Govindharajan, and Karthikeyan Ayyasamy. "Artificial Intelligence-Powered Intelligent Reflecting Surface Systems Countering Adversarial Attacks in Machine Learning." International Journal of Reconfigurable and Embedded Systems 13, no. 2 (2024): 414.

[4] Olutimehin, Abayomi Titilola, Adekunbi Justina Ajayi, Olufunke Cynthia Metibemu, Adebayo Yusuf Balogun, Tunboson Oyewale Oladoyinbo, and Oluwaseun Oladeji Olaniyi. "Adversarial Threats to AI-Driven Systems: Exploring the Attack Surface of Machine Learning Models and Countermeasures." Available at SSRN 5137026 (2025).

[5] Papangelo, Lorenzo, Maurizio Pistilli, Savio Sciancalepore, Gabriele Oligeri, Giuseppe Piro, and Gennaro Boggia. "Adversarial Machine Learning for Image-Based Radio Frequency Fingerprinting: Attacks and Defenses." IEEE Communications Magazine 62, no. 11 (2024): 108-113.

[6] Aiswerya, S. B., and S. Joseph Jawhar. "Detecting Complex Copy-Move Forgery Using KeyPoint-Siamese Capsule Network Against Adversarial Attacks." International Journal of Machine Learning and Cybernetics 16, no. 3 (2025): 1927-1953.

[7] Sun, Ruijin, Nan Cheng, Changle Li, Wei Quan, Haibo Zhou, Ying Wang, Wei Zhang, and Xuemin Shen. "A Comprehensive Survey of Knowledge-Driven Deep Learning for Intelligent Wireless Network Optimization in 6G." IEEE Communications Surveys & Tutorials (2025): 1099- 1135.

[8] Albalawi, Tahani, Perumal Ganeshkumar, and Faisal Albalwy. "Strategic Network Attack Prevention System Leveraging Sophisticated Query-Based Network Attention Algorithm (QNAA) And Self-Perpetuating Generative Adversarial Network (SPF-GAN) Techniques for Optimal Detection." Electronics 14, no. 5 (2025): 922.

[9] Rezaei, Hadiseh, Rahim Taheri, and Mohammad Shojafar. "FedLLMGuard: A Federated Large Language Model for Anomaly Detection In 5G Networks." Computer Networks 269 (2025): 111473.

[10] Ayanoglu, Ender, Kemal Davaslioglu, and Yalin E. Sagduyu. "Machine Learning In NextG Networks via Generative Adversarial Networks." IEEE Transactions on Cognitive Communications and Networking 8, no. 2 (2022): 480-501.

[11] Bamber, Sukhvinder Singh, Aditya Vardhan Reddy Katkuri, Shubham Sharma, and Mohit Angurala. "A Hybrid CNN-LSTM Approach for Intelligent Cyber Intrusion Detection System." Computers & Security 148 (2025): 104146.

[12] Yu, JianTong, and Li Li. "Research on 5G User Perception Detection and Experience Improvement Optimization Based on Capsule Network." International Journal of Interdisciplinary Telecommunications and Networking (IJITN) 16, no. 1 (2024): 1-20.

[13] Li, Yueqiao, Hang Su, and Jun Zhu. "AdvCapsNet: To Defense Adversarial Attacks Based on Capsule Networks." Journal of Visual Communication and Image Representation 75 (2021): 103037.

[14] Gufran, Danish, Pooja Anandathirtha, and Sudeep Pasricha. "Sentinel: Securing indoor Localization Against Adversarial Attacks with Capsule Neural Networks." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 43, no. 11 (2024): 4021-4032.

[15] Alsharaiah, Mohammad A., Mohammed Amin Almaiah, Mansour Obeidat, and Rami Shehab. "Capsule Network Model for Detecting Spoofing Attack in the Internet of Medical Things (IoMT)." Iraqi Journal for Computer Science and Mathematics 6, no. 3 (2025): 35.

[16] Zanini, Samuele, Stefania Bartoletti, Giulia Focarelli, Ivan Palama, and Giuseppe Bianchi. "Location Security in 5G and Beyond: Potential Threats and Countermeasures." IEEE Communications Magazine (2026).

[17] Alla, Ildi, and Valeria Loscri. "Sec5GLoc: Securing 5G Indoor Localization via Adversary-Resilient Deep Learning Architecture." In 2025 IEEE Conference on Communications and Network Security (CNS), IEEE, 2025, 1-9.

[18] Wang, Yulong, Tong Sun, Shenghong Li, Xin Yuan, Wei Ni, Ekram Hossain, and H. Vincent Poor. "Adversarial Attacks and Defenses in Machine Learning-Empowered Communication Systems and Networks: A Contemporary Survey." IEEE Communications Surveys & Tutorials 25, no. 4 (2023): 2245-2298.

[19] Ilahi, Inaam, Muhammad Usama, Junaid Qadir, Muhammad Umar Janjua, Ala Al-Fuqaha, Dinh Thai Hoang, and Dusit Niyato. "Challenges and Countermeasures for Adversarial Attacks on Deep Reinforcement Learning." IEEE Transactions on Artificial Intelligence 3, no. 2 (2021): 90-109.

[20] Sreekala, Keshetti, C. Pretty Diana Cyril, S. Neelakandan, Saravanan Chandrasekaran, Ranjan Walia, and Eric Ofori Martinson. "Capsule Network-Based Deep Transfer Learning Model for Face Recognition." Wireless Communications and Mobile Computing 2022, no. 1 (2022): 2086613.

[21] Khaleel, Yahya Layth, Mustafa Abdulfattah Habeeb, Ahmed Shihab Albahri, Tahsien Al-Quraishi, Osamah Shihab Albahri, and Abdullah Hussein Alamoodi. "Network and Cybersecurity Applications of Defense in Adversarial Attacks: A State-of-the-Art Using Machine Learning and Deep Learning Methods." Journal of Intelligent Systems 33, no. 1 (2024): 20240153.

[22] Sasi, Tinshu, Arash Habibi Lashkari, Rongxing Lu, Pulei Xiong, and Shahrear Iqbal. "An Efficient Self Attention-Based 1D-CNN-LSTM Network for IoT Attack Detection and Identification Using Network Traffic." Journal of Information and Intelligence (2024): 375-400.

[23] Li, Xingwang, Yuan Gao, Ming Zeng, Xianfu Lei, Wanming Hao, Arumugam Nallanathan, and Octavia A. Dobre. "Recent Advances in Resource Allocation and Beam Prediction for Large Language Models Empowered ISAC Systems." IEEE Communications Magazine (2026) 113-119.

[24] B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek and S. Ulukus, "Channel-Aware Adversarial Attacks Against Deep Learning-Based Wireless Signal Classifiers," in IEEE Transactions on Wireless Communications, vol. 21, no. 6, June 2022, 3868-3880.

[25] Shihab, Mustafa Abdmajeed, Haydar Abdulameer Marhoon, Saadaldeen Rashid Ahmed, Ahmed Dheyaa Radhi, and Ravi Sekhar. "Towards Resilient Machine Learning Models: Addressing Adversarial Attacks in Wireless Sensor Network." Journal of Robotics and Control (JRC) 5, no. 5 (2024): 1599-1617.

[26] Zhang, Chaoyun, Paul Patras, and Hamed Haddadi. "Deep Learning in Mobile and Wireless Networking: A Survey." IEEE Communications surveys & tutorials 21, no. 3 (2019): 2224-2287.

[27] Parasuraman, Manikandan, Ramesh Sekaran, Suthendran Kannan, Vinayakumar Ravi, and Tahani Jaser Alahmadi. "An Optimized Transmission Mechanism for Mitigating Jamming Attacks in Multi-Hop Wireless Networks." International Journal of Sensors, Wireless Communications and Control 15, no. 2 (2025): 117-132.

[28] Son, Bui Duc, Gaosheng Zhao, Trinh Van Chien, and Dong In Kim. "Secure Distributed RIS-MIMO Over Double Scattering Channels: Adversarial Attack, Defense, and SER Improvement." IEEE Transactions on Communications 74 (2025): 797-811.

[29] Zhang, Dingwen, Liangbo Cheng, Yi Liu, Xinggang Wang, and Junwei Han. "Mamba Capsule Routing Towards Part-Whole Relational Camouflaged Object Detection." International Journal of Computer Vision 133, no. 10 (2025): 7201-7221.

[30] Zahid, Mohammad, and Taran Singh Bharati. "Leveraging Machine Learning and Deep Learning in IoT Security: A Review." Security and Privacy 9, no. 1 (2026): e70144.

[31] Blessie, E. Chandra, Pethuru Raj, and B. Sundaravadivazhagan, eds. Generative Adversarial Networks for Cybersecurity:: Protecting Data and Networks. CRC Press, 2026.

[32] Ieropoulos, Vasilis, Eirini Anthi, Theodoros Spyridopoulos, Pete Burnap, Pietro Carnelli, and Aftab Khan. "Federated Detection at The Edge: Collaborative Anomaly Detection for Resource-Limited IoT." IEEE Internet of Things Journal (2026): 24205- 24218.

[33] Muthusundar, S. K., Nallusamy R, Shri Vindhya A, and Vignesh T. "Wireless Sensor Networks Security Using SACCGAN-RSA in a Novel Deep Learning–Based Intrusion Detection Framework for Enhancing." International Journal of Communication Systems 39, no. 4 (2026): e70397.

[34] Askhatuly, Aidos, Dinara Berdysheva, Azamat Berdyshev, Aigul Adamova, and Didar Yedilkhan. "Adversarial Attacks and Defense Mechanisms in Machine Learning: A Structured Review of Methods, Domains, and Open Challenges." IEEE Access (2025).

[35] 5G/6G Multipath Fading Equalization Dataset, Available online at: https://www.kaggle.com/datasets/programmer3/5g6g-multipath-fading-equalization-dataset, Last accessed on 31st May 2026.

[36] 6G Network Slice Security Attack Detection, Available online at: https://www.kaggle.com/datasets/ziya07/6g-network-slice-security-attack-detection, Last accessed on 31st May 2026.