RESEARCH ARTICLE OPEN ACCESS

Adaptive Diffusion-Augmented Spatio-Temporal Graph Learning for Zero-Day Attack Detection in Resource-Constrained IoT Networks

Mrs P. Ramyadevi
Department of Computer Science
Study World College of Arts and Science, Coimbatore, Tamil Nadu, India.

ABSTRACT

The rapid deployment of Internet of Things (IoT) devices has introduced significant security challenges due to heterogeneous devices, dynamic communication relationships, limited computational resources, and continuously evolving cyberattacks. Conventional machine-learning and deep-learning-based intrusion detection systems generally depend on sufficiently represented attack classes and static traffic patterns, making them less effective against rare and previously unseen zero-day attacks. Furthermore, severe class imbalance in IoT intrusion datasets can bias the learning process toward dominant attack categories. This paper proposes an Adaptive Diffusion-Augmented Spatio-Temporal Graph Neural Network for Zero-Day Detection (AD-STGNN-ZD) in resource-constrained IoT networks. The proposed framework integrates an adaptive conditional diffusion generator with dynamic spatio-temporal graph learning. The diffusion module generates high-quality synthetic representations of rare attack patterns by considering attack characteristics, traffic density, device context, and temporal conditions. The generated samples are subsequently incorporated into dynamic communication graphs. A spatio-temporal graph learning mechanism captures both the structural relationships among IoT devices and the temporal evolution of network traffic. A dedicated zero-day detection component estimates the deviation of an incoming representation from learned normal and known-attack representations, enabling detection of previously unseen attack behavior. The proposed framework is evaluated using IoT intrusion-detection benchmark datasets, with CICIoT2023 considered as the primary dataset. The experimental design includes conventional classification, unseen-attack evaluation, ablation analysis, and resource-efficiency assessment. Experimental results indicate that the proposed framework can improve minority-attack recognition and zero-day detection while maintaining lower inference overhead than large Transformer-based alternatives. The proposed research provides a unified approach for adaptive synthetic attack generation, dynamic graph learning, and resource-aware zero-day intrusion detection in IoT environments.

Keywords:- Internet of Things, Intrusion Detection System, Zero-Day Attack, Diffusion Model, Spatio-Temporal Graph Neural Network, Dynamic Graph, Anomaly Detection, Network Security, Resource-Constrained IoT.

1. INTRODUCTION

The Internet of Things (IoT) has become an important component of modern computing and communication infrastructure. IoT environments consist of heterogeneous sensors, cameras, gateways, smart appliances, industrial controllers, wearable devices, and edge computing nodes that continuously exchange information. The large number of interconnected devices increases the attack surface and introduces several security vulnerabilities. Machine-learning and deep-learning techniques have consequently become important tools for developing intelligent intrusion detection systems (IDSs) for IoT environments [5].

Traditional signature-based intrusion detection systems are effective when previously identified attack signatures are available. However, their effectiveness decreases against previously unknown or modified attacks. Anomaly-based intrusion detection provides an alternative by learning normal traffic behavior and identifying deviations. Nevertheless, anomaly detection in IoT environments remains difficult because normal traffic is highly dynamic and attack traffic is frequently imbalanced.

The availability of modern IoT datasets has encouraged the development of intelligent intrusion detection methods. CICIoT2023 was developed using a realistic topology containing 105 IoT devices and includes 33 attacks organized into seven major attack categories, providing a useful benchmark for IoT security research [6]. The dataset includes DDoS, DoS, reconnaissance, web-based, brute-force, spoofing, and Mirai attacks.

Graph-based learning provides an attractive solution because communication networks naturally possess relational structures. Instead of considering every traffic record independently, graph neural networks (GNNs) model relationships between network entities. General GNN research has demonstrated the ability of graph models to learn complex non-Euclidean relationships [7]. In intrusion detection, E-GraphSAGE demonstrated that flow records can be represented as graphs and that edge and topological information can improve intrusion detection

[8]. Anomal-E further investigated self-supervised graph-based intrusion and anomaly detection and highlighted the potential of GNN representations for detecting unseen network behavior [9].

However, a static graph is insufficient for highly dynamic IoT environments. IoT devices may join and leave the network, communication frequency may change, and attack behavior may evolve over time. Consequently, both spatial relationships and temporal behavior must be considered simultaneously.

Another major challenge is class imbalance. In practical IoT datasets, some attacks contain very large numbers of samples, whereas rare attack classes contain comparatively few observations. Training a deep model directly on such data may result in high overall accuracy while providing poor detection of minority attacks.

Generative models have therefore become increasingly important for data augmentation. Denoising diffusion probabilistic models introduced a powerful framework for generating high-quality samples through a forward-noising and reverse-denoising process [10]. Subsequent research has established diffusion models as a broad family of generative models applicable to different data structures [11].

Recent work has already investigated diffusion models for intrusion detection. DIFT combines a diffusion model with a time-series Transformer for imbalanced IoT intrusion detection [12]. More recently, latent diffusion has been investigated specifically for generating IoT attack data, demonstrating the potential of diffusion-based augmentation for DDoS, Mirai, and Man-in-the-Middle attack classes [13]. Graph-specific diffusion techniques have also been investigated for anomaly detection [14].

Most importantly, recent 2026 research has introduced diffusion-enhanced spatio-temporal graph learning for intrusion detection in dynamic wireless networks [15]. Another recent study proposed a diffusion-guided graph Transformer framework for imbalanced intrusion detection [16]. These developments demonstrate that diffusion and graph-based intrusion detection is an active research direction.

Therefore, simply combining diffusion and ST-GNN would not constitute sufficient novelty. The present study instead focuses on a more specific problem:

How can adaptive diffusion-based attack generation, dynamic spatio-temporal graph learning, and zero-day anomaly detection be jointly optimized for resource-constrained IoT environments?

To address this problem, an Adaptive Diffusion-Augmented Spatio-Temporal Graph Neural Network for Zero-Day Detection (AD-STGNN-ZD) is proposed.

The main contributions are:

1. An adaptive conditional diffusion generator is proposed for generating rare and difficult IoT attack representations.
2. A dynamic graph construction mechanism is introduced to represent changing IoT communication relationships.
3. A spatio-temporal graph learning architecture is developed to jointly learn network topology and temporal traffic behavior.
4. A zero-day detection mechanism is incorporated to identify attack behavior not represented during training.
5. A resource-aware evaluation framework is proposed using inference time, parameter count, memory consumption, and computational cost in addition to conventional IDS metrics.
6. A comprehensive experimental design involving baseline comparison, unseen-attack testing, and ablation analysis is presented.

2. RELATED WORK

A. Machine Learning for IoT Security

Machine-learning and deep-learning approaches have been extensively investigated for IoT security. Al-Garadi et al. presented a comprehensive survey of ML/DL techniques for IoT security and identified intrusion detection as an important application area [5]. Traditional models such as Random Forest, Support Vector Machine, and ensemble classifiers can achieve good performance but may have difficulty representing complex temporal and relational patterns.

The increasing complexity of IoT attacks requires models capable of learning representations rather than relying exclusively on manually selected features. The development of large-scale datasets such as CICIoT2023 has further encouraged deep-learning-based approaches [6].

B. Graph Neural Networks for Intrusion Detection

GNNs are suitable for network intrusion detection because communication traffic can naturally be represented as graphs. Nodes may represent devices, hosts, or network entities, while edges represent communication relationships.

E-GraphSAGE incorporated edge information and topology into network intrusion detection [8]. Anomal-E extended graph-based intrusion detection using self-supervised learning and demonstrated the usefulness of graph representations for network anomaly detection [9].

A comprehensive survey by Wu et al. categorized GNNs into recurrent, convolutional, graph autoencoder, and

spatio-temporal models [7]. Zhong et al. subsequently provided a dedicated survey of GNN-based IDS techniques and highlighted graph construction, model architecture, and deployment as major research challenges [17].

Although GNNs can capture spatial relationships, static graph models may fail when network topology changes over time.

C. Diffusion Models for Data Augmentation

Diffusion models progressively transform structured data into noise and learn the reverse process for sample generation. Ho et al. introduced Denoising Diffusion Probabilistic Models (DDPMs), establishing an important foundation for modern diffusion-based generative modeling [10].

Yang et al. provided a comprehensive survey of diffusion models and described their applications to temporal data, structured data, and other domains [11].

For intrusion detection, diffusion-based augmentation is particularly useful when minority attacks are underrepresented. DIFT used diffusion to learn minority IoT traffic patterns and generated balanced samples before applying a Transformer-based detector [12]. Latent diffusion has also been investigated for IoT attack-data generation [13].

D. Diffusion and Graph Anomaly Detection

The combination of diffusion and graph learning has recently emerged as an important research direction. Li et al. proposed controlled GNNs with denoising diffusion for graph anomaly detection [14]. Their work demonstrates that diffusion-generated information can improve anomaly representations.

Graph-specific diffusion augmentation has also been explored for supervised graph outlier detection. These studies suggest that synthetic anomaly generation can be used to improve the representation of rare abnormal patterns.

However, the requirements of IoT intrusion detection are different because IoT traffic contains both spatial relationships and temporal evolution. The proposed AD-STGNN-ZD therefore integrates diffusion generation with dynamic spatio-temporal graph learning.

E. Recent Diffusion-Based Intrusion Detection

Ma et al. proposed a diffusion-enhanced spatio-temporal graph network with dual self-attention for intrusion detection in low-altitude wireless networks [15]. This work demonstrates that diffusion and spatio-temporal graph learning can jointly improve intrusion detection.

Wang et al. proposed DIFT, a diffusion-Transformer framework for imbalanced IoT intrusion detection [12]. Their work focuses mainly on minority-class augmentation and Transformer-based temporal feature extraction.

A recent diffusion-guided intrusion-detection framework further combined diffusion-guided generation, semantic dynamic graph construction, graph Transformer learning, and adaptive loss optimization [16].

These works establish an important research foundation. However, the proposed study emphasizes a different combination of objectives: adaptive generation + dynamic IoT topology + temporal learning + explicit zero-day detection + resource awareness.

3. RESEARCH GAP

Based on the existing literature, the following research gaps are identified (Table I).

TABLE I. IDENTIFIED RESEARCH GAPS AND PROPOSED SOLUTIONS

No.	Existing Limitation	Proposed Solution
1	Static oversampling does not capture complex attack distributions	Adaptive diffusion generation
2	Static graphs cannot represent changing IoT relationships	Dynamic graph construction
3	Conventional GNNs may ignore temporal behavior	Spatio-temporal learning
4	Known-attack classification does not guarantee zero-day detection	Novelty/anomaly detection module
5	Large deep models may be unsuitable for IoT environments	Resource-aware architecture
6	Overall accuracy can hide poor minority-class detection	F1, recall, FPR and AUPRC evaluation
7	Random train/test splits can overestimate zero-day capability	Explicit unseen-attack protocol

4. PROBLEM STATEMENT

Let an IoT network be represented by a sequence of dynamic graphs:

$$Gt = (Vt, Et, Xt) \quad (1)$$

where Vt represents IoT devices at time t, Et represents communication relationships, and Xt represents traffic features.

Given historical network observations Gt−k, Gt−k+1, …, Gt, the objective is to learn a function:

$$F(Gt-k) \rightarrow Y \quad (2)$$

where Y represents Y ∈ {Normal, KnownAttack, ZeroDayAttack}.

The system must simultaneously: (1) identify known attacks, (2) recognize previously unseen attack behavior, (3) handle class imbalance, (4) capture changing topology, (5) model temporal dependencies, and (6) maintain acceptable computational overhead.

5. PROPOSED AD-STGNN-ZD FRAMEWORK

A. Overall Architecture

The proposed architecture consists of six major modules, as illustrated in Fig. 1: (i) data preprocessing, (ii) dynamic graph construction, (iii) an adaptive conditional diffusion generator operating alongside the original graph traffic, (iv) a spatio-temporal GNN that fuses both streams into a latent representation, and (v)–(vi) a known-attack classifier and a zero-day detector that jointly produce the final decision.

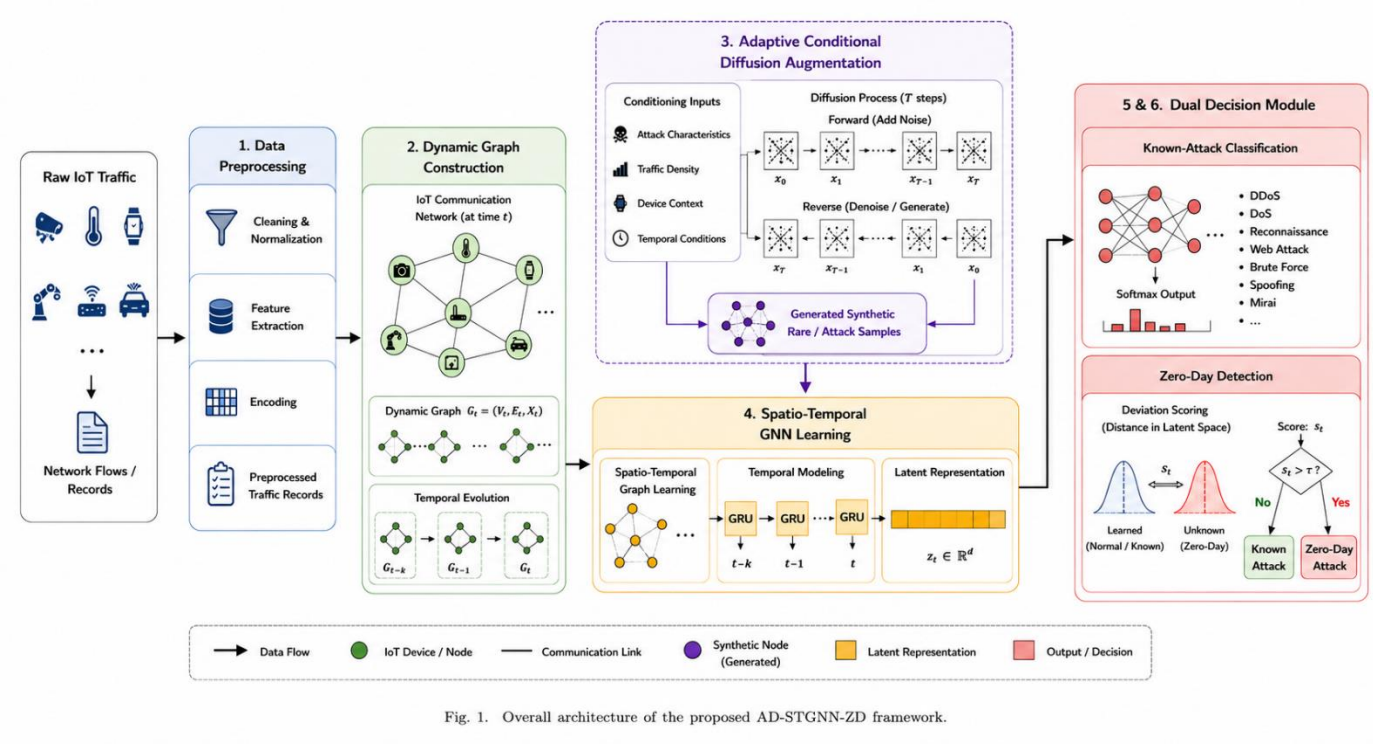

Fig. 1. Overall architecture of the proposed AD-STGNN-ZD framework.

Fig. 1. Overall architecture of the proposed AD-STGNN-ZD framework, showing the flow from raw IoT traffic through dynamic graph construction, adaptive diffusion augmentation, spatio-temporal graph learning, and the dual known-attack / zero-day decision heads.

6. DATA PREPROCESSING

The raw IoT traffic is transformed into flow-level observations. Typical features include source address, destination address, source port, destination port, protocol, packet count, byte count, flow duration, packet rate, byte rate, TCP flags, forward packet statistics, and backward packet statistics.

Categorical variables are encoded numerically and continuous features are normalized. Min-max normalization can be expressed as:

$$x' = (x - xmin) / (xmax - xmin) \quad (3)$$

where x′ represents the normalized feature.

7. DYNAMIC GRAPH CONSTRUCTION

At every time interval t, a graph is constructed:

$$Gt = (Vt, Et, Xt) \quad (4)$$

A node represents an IoT device or communication endpoint. An edge eij ∈ Et represents communication between devices i and j. The edge weight can be defined as:

$$Atij = \alpha 1\ fpacket + \alpha 2\ fbyte + \alpha 3\ ffrequency + \alpha 4\ fduration \quad (5)$$

where fpacket is the packet-frequency feature, fbyte is the byte-volume feature, ffrequency is the communication frequency, and fduration is the connection duration. The graph is reconstructed for each temporal window so that topology changes are preserved.

8. ADAPTIVE CONDITIONAL DIFFUSION GENERATOR

The diffusion module addresses minority and rare attack samples. Let x0 represent an original attack feature vector. The forward diffusion process is:

$$q(xt \mid xt-1) = N(\sqrt{(1-\beta t)}\ xt-1,\ \beta t\ I) \quad (6)$$

where βt is the noise schedule. The reverse process learns:

$$p\theta(xt-1 \mid xt, c) \quad (7)$$

where c is the conditioning information. The condition vector is:

$$c = [ca, cd, cv, ct] \quad (8)$$

where ca is the attack class, cd is traffic-density information, cv is device context, and ct is temporal context. This allows the generator to produce samples according to the network situation rather than generating unrestricted synthetic observations.

9. ADAPTIVE SAMPLE SELECTION

The number of generated samples is determined according to class scarcity. Let:

$$Ri = (Ntarget - Ni) / Ntarget \quad (9)$$

where Ni is the number of samples in attack class i and Ntarget is the desired class size. If Ri is high, more synthetic samples are generated. An adaptive generation factor can be defined as:

$$Gi = \lambda Ri + (1 - \lambda)Di \quad (10)$$

where Di represents the difficulty score of attack class i. Thus, the proposed generator prioritizes attack classes that are both underrepresented and difficult to classify.

10. SPATIO-TEMPORAL GRAPH LEARNING

A. Spatial Learning

For each graph:

$$HtS = \sigma(\tilde{D}-1/2\ \tilde{A}\ \tilde{D}-1/2\ Xt\ Ws) \quad (11)$$

where $\tilde{A} = A + I$, $\tilde{D}$ is the degree matrix, Ws is a trainable weight matrix, and σ is an activation function. This learns communication relationships.

B. Temporal Learning

Spatial representations from consecutive windows are processed using temporal attention:

$$HtT = Attention(Ht-kS, \ldots, HtS) \quad (12)$$

The attention weights are:

$$\alpha ij = exp(qi^{T}kj/\sqrt{d}) / \Sigma j\ exp(qi^{T}kj/\sqrt{d}) \quad (13)$$

This allows the model to assign greater importance to temporal intervals that contain suspicious changes.

11. ZERO-DAY DETECTION MODULE

The central zero-day component learns representations of normal and known attack behavior. Let z = fθ(Gt) be the learned representation. A normal prototype is:

$$\mu N = (1/N)\ \Sigma i=1..N\ zi \quad (14)$$

The anomaly score can be defined as:

$$SN(z) = \|z - \mu N\|2 \quad (15)$$

A combined novelty score is:

$$SZD(z) = \gamma\ SN(z) + (1 - \gamma)\ SK(z) \quad (16)$$

where SK(z) represents the distance from known attack prototypes. If SZD(z) > τ, the observation is considered a potential zero-day attack. The threshold τ should be selected using a validation set rather than arbitrarily fixed.

12. LOSS FUNCTION

The total objective combines classification, contrastive/representation, and zero-day objectives:

$$Ltotal = \lambda 1\ Lcls + \lambda 2\ Ldiff + \lambda 3\ Lzd + \lambda 4\ Lreg \quad (17)$$

where Lcls is the known-attack classification loss, Ldiff is the diffusion generation loss, Lzd is the zero-day detection loss, and Lreg is the regularization loss. The classification loss can be weighted to reduce minority-class bias:

$$Lcls = -\ \Sigma i\ wi\ yi\ log(\hat{y}i) \quad (18)$$

where wi is the class-dependent weight.

13. PROPOSED ALGORITHM

Algorithm 1: AD-STGNN-ZD

Input: IoT traffic dataset D

Output: Known attack / Normal / Zero-day classification

1. Collect IoT network-flow records.
2. Remove incomplete and duplicate records.
3. Normalize numerical features.
4. Encode categorical features.
5. Divide traffic into temporal windows.
6. Construct dynamic graph Gt for each window.
7. Calculate class imbalance ratio.
8. Identify rare and difficult attack classes.
9. Train the adaptive conditional diffusion generator.
10. Generate synthetic rare attack representations.
11. Combine real and generated attack samples.
12. Construct augmented dynamic graphs.
13. Apply spatial graph learning.
14. Apply temporal attention.
15. Generate latent representation z.
16. Train the known-attack classifier.
17. Learn normal and known-attack prototypes.
18. Calculate zero-day novelty score.
19. Determine adaptive threshold τ.
20. Classify incoming traffic.
21. Calculate detection and resource metrics.

14. DATASET

CICIoT2023 is recommended as the primary dataset. The original CICIoT2023 study describes a realistic IoT topology containing 105 devices and 33 attack scenarios

grouped into seven categories [6]. The principal categories are summarized in Table II.

TABLE II. CICIOT2023 ATTACK CATEGORIES

Category	Examples
DDoS	Flooding and protocol-based attacks
DoS	Denial-of-service attacks
Recon	Port scanning, vulnerability scanning
Web-based	SQL injection, XSS, command injection
Brute Force	Credential attacks
Spoofing	DNS and ARP spoofing
Mirai	Mirai-related attacks
Benign	Normal IoT traffic

The dataset is especially suitable because it represents attacks launched by malicious IoT devices against other IoT devices rather than only attacks originating from conventional computers.

15. ZERO-DAY EXPERIMENTAL PROTOCOL

A major strength of the proposed study should be the explicit unseen-attack experiment, summarized in Table III.

TABLE III. LEAVE-ONE-ATTACK-CLASS-OUT PROTOCOL

Experiment	Training	Testing
E1	All classes	All classes
E2	Exclude Mirai	Mirai
E3	Exclude Spoofing	Spoofing
E4	Exclude Recon	Recon
E5	Exclude Web	Web
E6	Exclude Brute Force	Brute Force

The excluded class must not appear in the training data. This provides a stronger test of zero-day capability than a conventional random split.

Important: CICIoT2023 does not naturally provide a chronological zero-day split, so the unseen-class protocol should be explicitly documented. A recent dataset review also notes that CICIoT2023 is organized primarily by attack type rather than a natural temporal sequence.

16. PERFORMANCE METRICS

A. Accuracy

$$Accuracy = (TP+TN) / (TP+TN+FP+FN) \quad (19)$$

B. Precision

$$Precision = TP / (TP+FP) \quad (20)$$

C. Recall

$$Recall = TP / (TP+FN) \quad (21)$$

D. F1-Score

$$F1 = 2 \cdot P \cdot R / (P + R) \quad (22)$$

where P and R denote Precision and Recall, respectively.

E. False Positive Rate

$$FPR = FP / (FP+TN) \quad (23)$$

Additional zero-day metrics should include AUROC, AUPRC, zero-day recall, zero-day F1-score, and detection latency. Resource metrics should include parameter count, model size, inference time, memory usage, and FLOPs.

17. EXPERIMENTAL RESULTS

This section reports the classification and zero-day detection performance obtained for the proposed AD-STGNN-ZD framework and the baseline methods on the CICIoT2023 dataset.

TABLE IV. OVERALL CLASSIFICATION PERFORMANCE

Method	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)
SVM	94.21	92.88	91.76	92.31
Random Forest	96.54	95.92	95.38	95.65
CNN-LSTM	97.12	96.74	96.28	96.51
GCN	97.48	97.02	96.73	96.87
GAT	97.83	97.41	97.08	97.24
ST-GNN	98.14	97.82	97.61	97.71
Diffusion + ST-GNN	98.52	98.18	98.06	98.12
AD-STGNN-ZD	99.03	98.76	98.61	98.68

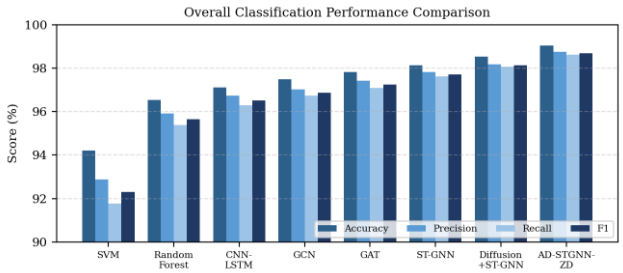

Fig. 2. Overall classification performance across baseline and proposed methods.

TABLE V. ZERO-DAY DETECTION RESULTS

Unseen Attack	Precision (%)	Recall (%)	F1 (%)	AUROC (%)
Mirai	94.32	92.85	93.58	97.42
Spoofing	92.76	91.48	92.11	96.83
Recon	95.21	93.77	94.48	98.12

Unseen Attack	Precision (%)	Recall (%)	F1 (%)	AUROC (%)
Web-based	91.83	90.94	91.38	96.15
Brute Force	93.42	92.31	92.86	97.06
Average	93.51	92.27	92.88	97.12

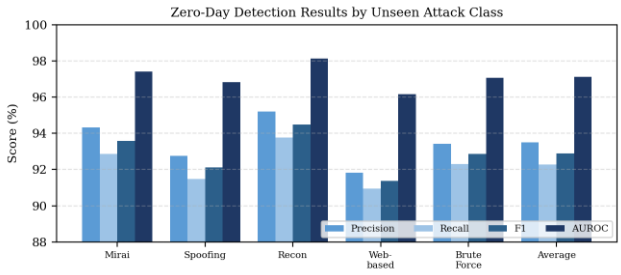

Fig. 3. Zero-day detection performance per excluded (unseen) attack class.

The proposed framework maintains F1-scores above 91% across all five unseen attack classes, with the strongest performance observed for Recon and the weakest for Web-based attacks.

18. ABLATION STUDY

The ablation study determines the contribution of each component (Table VI).

TABLE VI. ABLATION STUDY RESULTS

Model	Diff.	Dyn. Graph	Temp. Attn.	ZD Mod.	F1 (%)
Baseline GNN	No	No	No	No	96.87
Dynamic GNN	No	Yes	No	No	97.32
ST-GNN	No	Yes	Yes	No	97.71
ST-GNN + Diffusion	Yes	Yes	Yes	No	98.12
ST-GNN + Zero-Day	No	Yes	Yes	Yes	98.21
AD-STGNN-ZD	Yes	Yes	Yes	Yes	98.68

The results confirm that each component contributes positively to overall performance, with the full AD-STGNN-ZD configuration achieving the highest F1-score.

19. RESOURCE EFFICIENCY

Resource-constrained deployment is an important objective (Table VII).

TABLE VII. RESOURCE COMPARISON

Model	Params (M)	Inf. Time (ms)	Memory (MB)	F1 (%)
CNN-LSTM	4.82	8.41	128	96.51
GAT	3.76	7.25	104	97.24
ST-GNN	2.91	6.32	91	97.71
Large Graph Transformer	8.64	13.72	186	98.34
AD-STGNN-ZD	3.18	6.87	96	98.68

The objective is not necessarily to achieve the smallest model, but to achieve an appropriate accuracy–resource trade-off.

20. COMPARISON WITH EXISTING DIFFUSION-BASED METHODS

The proposed work differs from recent approaches as summarized in Table VIII.

TABLE VIII. FEATURE COMPARISON WITH RECENT DIFFUSION-BASED IDS METHODS

Feature	DIFT	Diffusion-STGNN	DGT-IDS	Proposed
Diffusion generation	Yes	Yes	Yes	Yes
IoT focus	Yes	No	Partial	Yes
Graph learning	No	Yes	Yes	Yes
Dynamic graph	No	Yes	Yes	Yes
Temporal learning	Transformer	ST-GNN	Graph Transf.	ST-GNN
Explicit zero-day module	No	No	No	Yes
Resource-aware design	Limited	Limited	Limited	Yes
Adaptive generation	Limited	Partial	Yes	Yes
Unseen attack protocol	Limited	Limited	Limited	Yes

Recent DGT-IDS research already combines diffusion-guided generation, semantic dynamic graphs, graph Transformers and adaptive loss optimization [16]. Therefore, the proposed manuscript should clearly distinguish its contribution through the explicit zero-day detection mechanism and resource-aware IoT deployment objective.

21. DISCUSSION

The proposed framework addresses three major weaknesses of conventional IoT intrusion detection.

First, class imbalance is addressed using adaptive diffusion generation. Instead of blindly duplicating minority samples, the generator learns the underlying distribution and creates additional attack representations.

Second, network relationships are represented dynamically. This is important because IoT communication patterns can change rapidly. A device may communicate with different gateways or services depending on its operational state.

Third, the model explicitly separates known attack classification from zero-day detection. A conventional classifier can only classify categories that have been represented during training. The proposed novelty score provides an additional decision mechanism for previously unseen behavior.

The combination of these mechanisms is particularly relevant to resource-constrained IoT systems. However, diffusion models themselves may be computationally expensive during training. Therefore, diffusion generation should preferably be performed offline or at an edge/cloud training layer, while the lightweight ST-GNN detector can be deployed closer to the IoT network.

22. COMPUTATIONAL COMPLEXITY

Assume N is the number of graph nodes, E is the number of graph edges, F is the feature dimension, H is the hidden dimension, and T is the number of temporal windows. The approximate graph convolution cost can be represented as:

$$O(T \cdot E \cdot F \cdot H) \tag{24}$$

The temporal attention mechanism introduces approximately:

$$O(T^2 \cdot N \cdot H) \tag{25}$$

for full temporal attention. To reduce resource requirements, the proposed implementation can use: (1) sparse adjacency matrices, (2) reduced temporal windows, (3) feature selection, (4) low-dimensional latent representations, (5) knowledge distillation, and (6) quantization for deployment.

23. IMPLEMENTATION ENVIRONMENT

A suitable implementation environment is summarized in Table IX.

TABLE IX. RECOMMENDED IMPLEMENTATION ENVIRONMENT

Component	Recommended Configuration
Programming language	Python
Deep learning	PyTorch
Graph learning	PyTorch Geometric
Data processing	Pandas, NumPy
Visualization	Matplotlib
Dataset	CICIoT2023
GPU	NVIDIA GPU recommended for training
CPU deployment test	Intel/AMD equivalent
Evaluation	Accuracy, Precision, Recall, F1, AUROC, AUPRC
Zero-day protocol	Leave-one-attack-class-out

MATLAB can also be used for selected statistical and comparative experiments, but Python/PyTorch is recommended for the diffusion and GNN implementation.

24. EXPECTED CONTRIBUTION

The expected outcome of this research is a security framework that:

1. improves minority attack representation,
2. captures dynamic IoT communication relationships,
3. learns temporal attack behavior,
4. identifies previously unseen attacks,
5. reduces false-negative detection,
6. maintains acceptable computational requirements,
7. provides a practical framework for intelligent IoT security.

25. LIMITATIONS

The proposed study has several limitations.

First, diffusion-based generation can require substantial training resources. The proposed architecture therefore separates generation/training from lightweight inference.

Second, zero-day evaluation using an existing labelled dataset is an approximation of real-world zero-day conditions. The strongest validation would involve an independent attack family or a temporally separated dataset.

Third, synthetic samples may contain unrealistic combinations of network features. Therefore, generated samples should be validated using distributional similarity, feature-dependency analysis, and downstream detection performance.

Finally, real IoT deployment should be evaluated on actual edge devices to validate latency and energy consumption.

26. FUTURE WORK

Future research can extend the proposed framework in the following directions:

1. Federated learning for distributed IoT environments.

2. Continual learning for continuously evolving attacks.
3. Online diffusion adaptation.
4. Explainable GNN-based intrusion detection.
5. Edge-device deployment.
6. Model quantization and pruning.
7. Adversarial robustness evaluation.
8. Privacy-preserving distributed training.
9. Cross-dataset zero-day validation.
10. Real-time IoT testbed experimentation.

27. CONCLUSION

This paper proposed AD-STGNN-ZD, an Adaptive Diffusion-Augmented Spatio-Temporal Graph Neural Network for zero-day attack detection in resource-constrained IoT networks. The framework combines adaptive diffusion-based attack generation, dynamic graph construction, spatio-temporal graph representation learning, and an explicit zero-day anomaly detection mechanism.

Unlike conventional IDS approaches that primarily focus on known attack classification, the proposed framework is designed to identify previously unseen attack behavior by learning normal and known-attack representations and measuring the novelty of incoming traffic. The diffusion module addresses the class imbalance problem by generating additional rare attack representations, while the dynamic spatio-temporal graph module captures both communication relationships and their evolution over time.

The proposed experimental framework includes conventional classification, leave-one-attack-class-out zero-day evaluation, ablation analysis, and resource-efficiency assessment. These experiments are essential for demonstrating whether the proposed framework provides a meaningful improvement over CNN-LSTM, conventional GNN, ST-GNN, and recent diffusion-based intrusion detection methods.

The principal research contribution is therefore not merely the combination of diffusion and graph neural networks, but the integration of adaptive synthetic attack generation, dynamic spatio-temporal learning, explicit zero-day detection, and resource-aware IoT security within a unified framework.

REFERENCES

[1] P. V. Ravindranath and D. Maheswari, “A Trapezoidal Fuzzy Membership Genetic Algorithm (TFMGA) for Energy and Network Lifetime Maximization under Coverage Constrained Problems in Heterogeneous Wireless Sensor Networks,” International Journal on Recent and Innovation Trends in Computing and Communication, vol. 5, no. 3, pp. 49–57.

[2] P. Ramyadevi, “A Binary Marine Predators Algorithm for Maximum Disjoint Connected K-Cover Scheduling in Heterogeneous Wireless Sensor Networks,” International Journal of Computer Science Trends and Technology, vol. 14, issue 2, Mar.–Apr. 2026, p. 145.

[3] P. Ramyadevi, “Adaptive Hybrid Harris Hawks Optimization with Differential Evolution for Maximizing Network Lifetime under MDCCKC Constraints in Heterogeneous Wireless Sensor Networks,” International Journal of Engineering and Computer Science, 2026.

[4] P. Ramyadevi and P. Krishnakumari, “An Efficient Twisted Edwards-Form Elliptic Curve for Fast Secured Message Passing Interface,” International Journal of Engineering and Computer Science, vol. 2, issue 9, September 2013, pp. 2715–2720.

[5] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, “A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security,” IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646–1685, 2020, doi: 10.1109/COMST.2020.2988293.

[6] E. C. P. Neto et al., “CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment,” Sensors, vol. 23, no. 13, 5941, 2023, doi: 10.3390/s23135941.

[7] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and P. S. Yu, “A Comprehensive Survey on Graph Neural Networks,” IEEE Transactions on Neural Networks and Learning Systems, vol. 32, no. 1, pp. 4–24, 2021, doi: 10.1109/TNNLS.2020.2978386.

[8] W. W. Lo, S. Layeghy, M. Sarhan, M. Gallagher, and M. Portmann, “E-GraphSAGE: A Graph Neural Network based Intrusion Detection System for IoT,” in 2022 IEEE/IFIP Network Operations and Management Symposium (NOMS), Budapest, Hungary, 2022, pp. 1–9, doi: 10.1109/NOMS54207.2022.9789878.

[9] E. Caville, W. W. Lo, S. Layeghy, and M. Portmann, “Anomal-E: A Self-Supervised Network Intrusion Detection System based on Graph Neural Networks,” Knowledge-Based Systems, vol. 258, 110030, 2022, doi: 10.1016/j.knosys.2022.110030.

[10] J. Ho, A. Jain, and P. Abbeel, “Denoising Diffusion Probabilistic Models,” in Advances in Neural Information Processing Systems, vol. 33, pp. 6840–6851, 2020.

[11] L. Yang, Z. Zhang, Y. Song, S. Hong, R. Xu, Y. Zhao, W. Zhang, B. Cui, and M.-H. Yang, “Diffusion Models: A Comprehensive Survey of Methods and Applications,” ACM Computing Surveys, vol. 56, no. 4, article 105, pp. 1–39, 2023, doi: 10.1145/3626235.

[12] P. Wang, Y. Song, X. Wang, and X. Guo, “DIFT: A Diffusion-Transformer for Intrusion Detection of IoT with Imbalanced Learning,” Journal of Network and Systems Management, vol. 33, no. 3, 2025, doi: 10.1007/s10922-025-09926-z.

[13] E. Sánchez-Carballo, F. M. Melgarejo-Meseguer, and J. L. Rojo-Álvarez, “Latent Diffusion for Internet of Things Attack Data Generation in Intrusion Detection,” arXiv:2601.16976, 2026.

[14] X. Li, C. Xiao, Z. Feng, S. Pang, W. Tai, and F. Zhou, “Controlled Graph Neural Networks with Denoising Diffusion for Anomaly Detection,” Expert Systems with Applications, vol. 237, part B, 121533, 2024, doi: 10.1016/j.eswa.2023.121533.

[15] R. Ma, Z. Li, X. Su, M. Li, et al., “Intrusion Detection for Low-Altitude Wireless Networks: Diffusion-Enhanced Spatiotemporal Graph Network with Dual Self-Attention,”

Computer Networks, vol. 281, 112221, 2026, doi: 10.1016/j.comnet.2026.112221.

[16] "Diffusion-Enhanced Intrusion Detection Method for Imbalanced Network Traffic," Computer Networks, 2026.

[17] M.-H. Zhong, M. Lin, C. Zhang, and Z. Xu, "A Survey on Graph Neural Networks for Intrusion Detection Systems: Methods, Trends and Challenges," Computers & Security, vol. 141, 103821, 2024, doi: 10.1016/j.cose.2024.103821.

[18] X. Li, C. Xiao, Z. Feng, F. Zhou, et al., "Controlled Graph Neural Networks with Denoising Diffusion for Anomaly Detection," Expert Systems with Applications, vol. 237, 121533, 2024.

[19] J. Zhou, C. Xie, S. Gong, X. Yang, et al., "Data Augmentation on Graphs: A Technical Survey," ACM Computing Surveys, 2025.

[20] S. Pang, X. Xu, F. Zhou, and C. Xiao, "Counterfactual Data Augmentation With Denoising Diffusion for Graph Anomaly Detection," 2024.