iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78908

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

A Comprehensive Survey on Deep Learning-Based DoS/DDoS Detection and Resource Management in 5G Network Slicing

Ambidi Naveena[1], Meghana Madipalli[2], Narayandas Shreya Vandana[3], Srivarsha Pochampally[4], Sneha Battula[5]
[1]*Associate Professor,* [2,3,4,5]*Student, 4th year, Department of Electronics and Telematics Engineering, G. Narayanamma Institute of Technology and Science, Affiliated by JNTUH, Hyderabad, India*

Abstract: ***With the rapid advancement of 5G communication technology, network slicing has emerged as a key enabler for supporting diverse applications with varying Quality of Service (QoS) requirements. It allows multiple virtual networks to operate on a shared physical infrastructure, ensuring efficient resource utilization and service flexibility. However, this flexibility also introduces significant security challenges, particularly from Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks that can disrupt services and degrade network performance. This paper presents a literature survey on network slicing, intrusion detection systems, deep learning- based attack detection, and intelligent resource allocation in 5G environments. Various techniques such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Reinforcement Learning (RL) are analyzed for traffic classification and attack mitigation. The study highlights their advantages, limitations, and identifies future directions for improving security and efficiency in 5G networks.***
Keywords: 5G Network Slicing, DoS/DDoS Detection, Deep Learning, Intrusion Detection System (IDS), Network Security

I. INTRODUCTION

The evolution of 5G communication networks has introduced network slicing as a fundamental concept that enables multiple virtual networks to operate over a shared physical infrastructure [12]. Each slice is designed to meet specific service requirements such as enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communication (uRLLC), and massive Machine-Type Communication (mMTC), improving flexibility and resource utilization. Despite its benefits, network slicing introduces new security challenges due to virtualization and shared resources. DoS and DDoS attacks can overwhelm network components and disrupt services across slices. To address these issues, machine learning and deep learning techniques are increasingly used for real-time attack detection and adaptive resource management, enhancing the overall reliability and security of 5G networks [13]. To better understand the existing solutions and research directions in this domain, the following section presents a detailed review of significant works focusing on deep learning-based attack detection and resource management in 5G network slicing.

II. LITERATURE SURVEY

A. Deep Learning-based Application Specific RAN Slicing for Mobile Networks

Du and Nakao [1] proposed a deep learning-based architecture for application-specific Radio Access Network (RAN) slicing. Their work focuses on improving resource allocation by identifying application types using a Deep Neural Network (DNN). This approach leverages packet header features such as IP address, port number, protocol, time-to-live, and packet size to classify applications without inspecting payloads, thereby preserving user privacy and reducing processing complexity.

Once classified, the system dynamically allocates radio resources based on application requirements. Real-time applications like video streaming and voice calls are prioritized over delay-tolerant services such as email. Experimental results demonstrated approximately 93.5% accuracy in identifying around 200 applications, showing that deep learning significantly improves spectrum efficiency [11] and enhances overall user experience in mobile networks.

B. Intrusion Detection System for 5G with a Focus on DoS and DDoS Attacks

Iashvili et al. [2] analyzed the vulnerabilities of 5G networks to DoS and DDoS attacks and proposed an Intrusion Detection System (IDS) tailored for 5G environments. The study highlights that traditional security mechanisms are insufficient due to the dynamic, virtualized nature of 5G networks enabled by SDN and NFV technologies [14].

The proposed IDS uses machine learning techniques to monitor traffic behaviour and detect anomalies based on features such as packet flow rate, traffic patterns, and connection behaviour. It can detect malicious activities in real time and integrate with the 5G core network for continuous monitoring, improving detection accuracy while reducing false positives and ensuring large-scale network security.

C. Deep Learning-based Approach for DDoS Detection and Mitigation in 5G

Bousalem et al. [3] proposed a deep learning-based system integrated with Software Defined Networking (SDN) to detect and mitigate DDoS attacks in 5G networks. The system uses a Convolutional Neural Network (CNN) to analyze network traffic patterns and classify them as benign or malicious.

Upon detecting an attack, the system isolates malicious users by assigning them to a low-resource "sinkhole" slice, preventing disruption to legitimate users. Experimental results showed about 97% detection accuracy, with a significant reduction in attacker throughput while maintaining stable performance for normal users, proving effective mitigation.

D. DeepSecure: Detection of DDoS Attacks on 5G Network Slicing

Kuadey et al. [4] introduced the DeepSecure framework, a deep learning-based approach using Long Short-Term Memory (LSTM) networks for DDoS detection in 5G network slicing. The framework includes an attack detection model and a slice prediction model for efficient traffic handling.

The detection model classifies traffic as normal or malicious, while the prediction model assigns legitimate traffic to appropriate slices. The system achieved 99.97% detection accuracy and 98.79% slice prediction accuracy, outperforming traditional models and demonstrating LSTM's strength in capturing temporal traffic patterns.

E. Secure Slicing Using Slice Isolation

Sattar and Matrawy [5] focused on enhancing security in network slicing by introducing slice isolation mechanisms. Their work highlights that DDoS attacks targeting one slice can affect others due to shared infrastructure, leading to performance degradation.

The proposed approach enforces isolation policies across different layers of the 5G core network to contain attack traffic within the affected slice. Experimental results show that slice isolation significantly reduces the impact of attacks, improving network reliability and ensuring service continuity.

F. Resource Allocation Using Reinforcement Learning

Liu et al. [6] proposed a constrained reinforcement learning approach for dynamic resource allocation in 5G network slicing. The system models the problem as a Constrained Markov Decision Process (CMDP), enabling adaptive decision- making based on network conditions.

The model considers parameters such as traffic load, bandwidth availability, and service requirements to allocate resources efficiently. Experimental results show improved throughput and reduced user dissatisfaction compared to traditional methods, proving the effectiveness of reinforcement learning in dynamic environments.

G. 5G Network Slicing: Multi-Tenancy Scenario

Oladejo and Falowo [7] studied network slicing in multi-tenant environments where multiple virtual operators share the same infrastructure. The paper addresses resource allocation challenges and proposes a hierarchical allocation model.

In this model, infrastructure providers allocate resources to operators, who further distribute them among slices. Slice prioritization ensures critical services receive sufficient resources. Simulation results show improved network capacity and fairness, highlighting efficient resource management.

H. Entropy-Based DDoS Detection in SDN

Ahalawat et al. [8] proposed an entropy-based approach for detecting DDoS attacks in OpenFlow-enabled SDN networks. The method analyzes traffic randomness using features like IP address, ports, and flow rate to identify abnormal behaviour.

When entropy values deviate from normal patterns, the system detects attacks and applies rate-limiting using OpenFlow meter tables. Experimental results show effective detection and mitigation, restoring bandwidth and CPU usage to normal levels.

I. *DeepDefense: Deep Learning for DDoS Detection*

Yuan et al. [9] proposed DeepDefense, a deep learning-based framework for detecting DDoS attacks. The model combines convolutional layers with recurrent neural networks to capture spatial and temporal features of traffic.

Evaluated on the ISCX2012 dataset, the model achieved higher accuracy and lower error rates compared to traditional methods. This demonstrates the advantage of deep learning in identifying complex attack patterns.

J. *End-to-End Network Slicing Architecture*

Nakao et al. [10] proposed an end-to-end network slicing architecture for 5G networks to support diverse QoS requirements. The framework divides the network into multiple virtual slices across RAN, core, and transport networks. By integrating SDN and NFV, the system enables dynamic resource allocation and flexible service deployment. Experimental results show improved scalability, flexibility, and isolation, making it essential for future 5G applications.

III. COMPARISON ANALYSIS

The reviewed papers employ various algorithms and methodologies to enhance network slicing performance and security. Deep learning models such as CNN and LSTM are widely used for traffic classification and DDoS detection due to their ability to learn complex patterns. CNN-based approaches achieve high accuracy in spatial feature extraction, while LSTM models effectively capture temporal dependencies in network traffic.

Reinforcement learning is applied for dynamic resource allocation, offering adaptability to changing network conditions. Architectural solutions such as slice isolation help prevent attack propagation across slices, while IDS-based approaches utilize machine learning for real-time anomaly detection. Although deep learning models provide high accuracy, they require large datasets and significant computational resources. In contrast, reinforcement learning and architectural methods improve efficiency but may introduce higher implementation complexity.

Overall, deep learning approaches, particularly CNN and LSTM, demonstrate strong performance in detecting complex attack patterns, whereas reinforcement learning offers adaptability in dynamic environments. However, the choice of method depends on trade-offs between accuracy, computational cost, and practical deployment. A comparison of machine learning and deep learning approaches in 5G network slicing and security is presented in Table 1.

TABLE I
Comparison of Machine Learning and Deep Learning Approaches in 5G Network Security and Slicing

Author	Method Used	Purpose	Advantages
Du & Nakao [1]	Deep Neural Network (DNN)	Application classification for RAN slicing	~93.5% accuracy, improved spectrum efficiency, better user experience
Iashvili et al. [2]	Machine Learning-based IDS	Intrusion detection in 5G	Real-time detection, reduced false positives, enhanced security
Bousalem et al. [3]	CNN + SDN	DDoS detection and mitigation	~97% accuracy, attack isolation, stable performance for normal users
Kuadey et al. [4]	LSTM (DeepSecure Framework)	DDoS detection and slice prediction	99.97% detection accuracy, 98.79% prediction accuracy
Sattar & Matrawy [5]	Slice Isolation Mechanism	DDoS mitigation in network slicing	Prevents attack spread, improves reliability and service continuity
Liu et al. [6]	Reinforcement Learning (CMDP)	Dynamic resource allocation	Improved throughput, reduced user dissatisfaction, adaptive decisions
Oladejo & Falowo [7]	Multi-tenant slicing model	Resource sharing in multi-tenant environments	Improved fairness, efficient resource use, increased network capacity
Ahalawat et al. [8]	Entropy-based detection + SDN	DDoS detection and mitigation	Effective anomaly detection, restores bandwidth and CPU usage
Yuan et al. [9]	Deep Learning (CNN + RNN)	DDoS detection	High accuracy, captures spatial & temporal patterns, low error rates
Nakao et al. [10]	SDN + NFV-based slicing architecture	End-to-end 5G network slicing	Improved scalability, flexibility, and slice isolation

IV. CONCLUSION

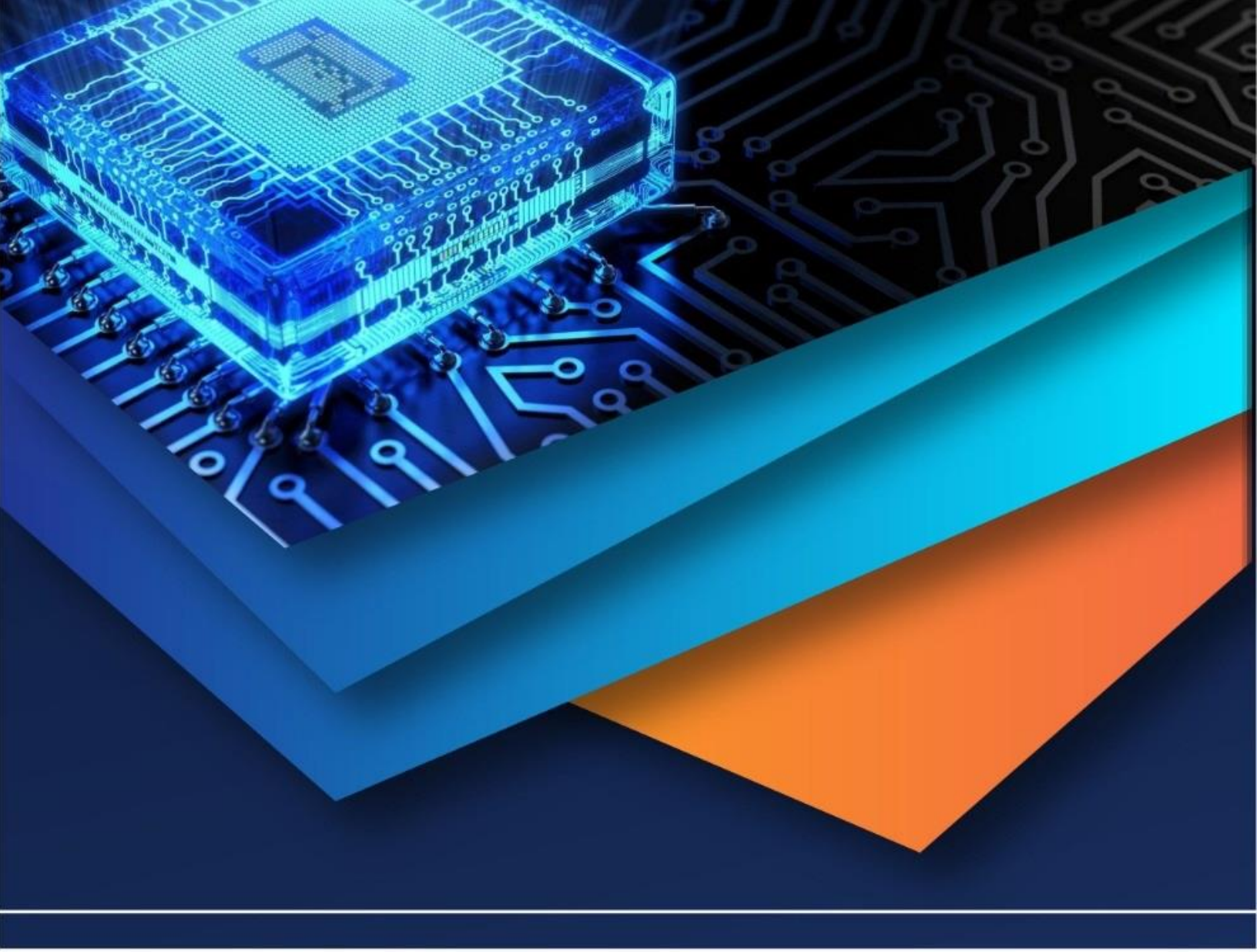
This literature survey highlights the significant role of deep learning and intelligent techniques in enhancing the security and efficiency of 5G network slicing. Approaches such as CNN, LSTM, reinforcement learning, and slice isolation mechanisms effectively improve DDoS detection, resource allocation, and overall network performance. Among these, deep learning models demonstrate high accuracy in identifying complex attack patterns, while reinforcement learning offers adaptability in dynamic network conditions. The integration of these techniques contributes to improved reliability, scalability, and service quality in modern 5G environments.

V. FUTURE SCOPE

Future work can focus on developing hybrid models that combine multiple deep learning techniques to improve detection accuracy and robustness. Real-time implementation in large-scale 5G networks and the development of more realistic, slice-aware datasets remain key challenges. Additionally, extending these models to handle diverse cyber threats and incorporating adaptive, self-learning mechanisms can further strengthen network security. Furthermore, the development of lightweight and computationally efficient models will be essential for real-time deployment in practical 5G network environments.

REFERENCES

[1] P. Du and A. Nakao, "Deep Learning-based Application Specific RAN Slicing for Mobile Networks," The University of Tokyo, Tokyo, Japan, IEEE, 2018.
[2] G. Iashvili, M. Iavich, R. Bocu, R. Odarchenko, and S. Gnatyuk, "Intrusion Detection System for 5G with a Focus on DoS/DDoS Attacks," International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), 2021, pp. 1–6.
[3] M. P. Novaes, L. F. Carvalho, E. R. Hruschka, and J. P. Papa, "Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment," IEEE Access, vol. 8, pp. 83765–83781, 2020.
[4] N. A. E. Kuadey, S. Khan, R. Ullah, and S. H. Ahmed, "DeepSecure: Detection of distributed denial of service attacks on 5G network slicing—Deep learning approach," IEEE Wireless Communications Letters, vol. 11, no. 3, pp. 488–492, Mar. 2022
[5] D. Sattar and A. Matrawy, "Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices", IEEE Conference on Communications and Network Security (CNS), 2020, pp. 1–9.
[6] Y. Liu, J. Ding, and X. Liu, " Resource Allocation Method for Network Slicing Using Constrained Reinforcement Learning," IFIP Networking Conference (IFIP Networking), 2021, pp. 1–3.
[7] S. O. Oladejo and O. E. Falowo, "5G Network Slicing: A Multi-Tenancy Scenario," Global Wireless Summit (GWS), 2017,
[8] pp. 88–92.
[9] A. Ahalawat, S. S. Dash, A. Panda, and K. S. Babu, "Entropy Based DDoS Detection and Mitigation in OpenFlow Enabled SDN," International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 2019,
[10] pp. 1–5.
[11] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS attack via deep learning," in 2017 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 1–8, 2017.
[12] P. Du and A. Nakao, "End-to-End Network Slicing for 5G Mobile Networks," IEEE Conference, University of Tokyo, Tokyo, Japan, 2018.
[13] X. Li et al., "Network Slicing for 5G: Challenges and Opportunities," IEEE Internet Computing, vol. 21, no. 5, 2017.
[14] T. Yoo, "Network Slicing Architecture for 5G Network," International Conference on Information and Communication Technology Convergence (ICTC), 2016, pp. 1010–1014.
[15] S. Wang, X. Zhang, Y. Zhang, et al., "A Survey on Mobile Edge Networks: Convergence of Computing, Caching and Communications," IEEE Access, 2017.
[16] D. Sattar and A. Matrawy, "Security in Software-Defined Networking: DDoS Detection and Mitigation," IEEE Confernece on Communications and Network Security (CNS), 2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY