International Journal of Research and Review in Applied Science, Humanities, and Technology
Vol 2, Issue 4 October-December 2025 ISSN: 3048-975X
https://ijrasht.com/

AI-Driven Intrusion Detection Framework for 5G and Beyond Networks

Nishtha, Assistant Professor, Maharaja Surajmal Institute of Technology, Delhi, India nishthasaroha@gmail.com

Vishakha Tomar, Assistant Professor, Maharaja Surajmal Institute of Technology, Delhi, India vishakhatomar@msit.in

Abstract: The evolution of wireless networks into the fifth generation (5G) and beyond has enabled unprecedented connectivity, very low latency, and an enormous density of devices. As much as these advances are positive to the new applications of smart cities, autonomous vehicles, and industrial IoT, it has also introduced more attack surfaces and vulnerabilities. The dynamic, high-throughput and decentralized nature of the 5G network is almost impossible to be supported by the legacy-based intrusion detection system (IDS). As a result, AI-based intrusion detecting systems are increasingly being considered as the future of cybersecurity systems. The current paper is a review and analysis of AI in IDS 5G and above networks. It explains the implementation of machine learning (ML), deep learning (DL), and reinforcement learning (RL) into intrusion detection to make it more adaptable, scalable, and more effective at detecting intrusions. The paper recognizes the following frameworks: anomaly-based IDS, federated learning-based IDS to maintain privacy, and hybrid AI-IDS models, that incorporates the signature-based and behaviours-based detection. Furthermore, it discusses how AI-based IDS can be used to slice networks, software-defined networking (SDN), and edge computing-enabled 5G networks. The findings indicate that artificial intelligence-based IDS can detect zero-day attacks, distributed denial-of-service (DDoS) and advanced persistent threats significantly better than conventional systems. Nevertheless, interpretability of models, inaccessible training data, the cost of computation and AI adversarial attacks remain a problem. Explainable AI (XAI), sparse models to support edge devices, and cross-layer collaborative intrusion detection are other issues that need to be studied to guarantee safe and reliable next-generation networks. In this paper, we find that AI-powered intrusion detection systems are both practical and warranted in providing cybersecurity in 5G and beyond ecosystems, the mainstay of secure digital infrastructure.

Keywords: Cybersecurity, Artificial Intelligence, technology intrusion detection, 5G networks.

1. Introduction

The growth of 5G and other networks will be more performance-focused in bandwidth, latency and scalability. But also networks can show the most sinister hue of the issues as they are not in the centre of and can bring more of the attacks to attack (Ali et al., 2021). The traditional IDS is limited to managing dynamic and sophisticated threats and is designed to be employed with a static and centralized architectural design. Both (ML and DL) have shown that a high level of automation of an intrusion detection process can be highly versatile and precise (Hussain et al., 2020). AI-based IDS can process high-dimensional traffic data, detect unrecognized patterns of attack and react to evolving threats. This makes the next-generation network a need-to-have AI integration.

2. Background of the Study

With the assistance of intrusion detection systems, malicious activities, including unauthorized access, malware propagation, and denial-of-service attacks can be detected. The signature-based detectives used in older versions of IDS cannot be effective in a zero-day attack (Kim et al., 2019). Adaptive and data-driven detection models have now become an urgent need as 5G emerges as a complex technology. Other AI-based models are currently being implemented to classify traffic using CNNs, forecast threats over time using RNNs, and automatically produce adaptable policies using RL in the context of IDS (Sharma et al., 2020). Federated learning is another privacy-preserving IDS training, which is performed on the distributed 5G nodes, to improve the security without sacrificing user information.

3. Justification

AI-led IDS needs justification in 5G due to three reasons. First, 5G network traffic is too high and too fast to be identified by hand or with rules (Ali et al., 2021). Second, despite the adversarial AI, it is impossible to provide guarantees that the increasing sophistication of cyberattacks can be matched by intelligent and adaptive protections (Hussain et al., 2020). Third, the data protection rule should include secure mechanisms that are user-privacy-efficient that trade off detection and user privacy.

As per the current and emerging threats, AI-based IDS is intelligent and adaptable, which the currently existing traditional IDS does not possess and can be scaled, predictive, and learn, one of the key features of the implementation of sustainable 5G.

4. Objectives of the Study

1. To test AI-powered intrusion detection processes in 5G and beyond networks.
2. In order to compare ML, DL and RL-based IDS models.
3. To experiment with problems such as adversarial attacks, data scarcity and computational cost.
4. To propose the future research direction in sustainable AI-ID in 5G ecosystems.

5. Literature Review

Intrusion Detection Systems (IDS) have always been a part of cybersecurity mechanisms. The heterogeneity of connected devices, their density, and complexity is now a novel challenge to IDS due to 5G networks. The studies of AI-based IDS have recognized that there are a number of strategies, and each strategy possesses its own strengths and limitations.

Signature vs Anomaly IDS: In traditional signature based IDS, attack signatures are used to identify intrusion. These systems are highly efficient to attack common threats and cannot recognize zero-day attacks and novel intrusions. On the other hand, anomaly-based IDS relies on AI to understand how networks should look and identify anomalies and can therefore react to new threats with less effort (Kim et al., 2019). However, due to the nature of normal traffic patterns, the false-positive of the anomaly-based systems is higher.

Machine Learning-based IDS: The literature on machine learning (ML) techniques (support vector machine, SVMs, randomly forest, and clustering models) to identify network traffic anomalies is substantial. The models can handle moderate complexity and are more accurate in their detection than signature-based IDS (Xia et al., 2020). They, however, are not easily scalable and do not support high-dimensional traffic information, which is typical of the 5G networks.

Deep Learning-based IDS: The intrusion detection systems have been enhanced with the transition into the field of deep learning (DL). The reason is that convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are the most appropriate tools to consider the high-dimensional nature of traffic and capture the temporal characteristics of 5G communication patterns (Hussain et al., 2020). DL-based IDS is useful to detect anomalies on-the-fly but is disadvantaged by both large computing footprint and reduced interpretability.

Federated IDS: Federated learning-based IDS has emerged as an attractive technology as the issue of data privacy continues to grow. The paradigm enables co-training of IDS models by two or more distributed 5G nodes, without transferring raw traffic data. Therefore, federated IDS is a chance to ensure users privacy and increase the detection rates of a heterogeneous network (Yang et al., 2021). However there are overhead communication and model synchronization issues.

Hybrid IDS Approaches: Hybrid IDS is a detection technique that combines AI-based anomaly detection with rule-based detection to reap the advantages of each technique. It is true as well since such systems would be able to detect the unfamiliar threats, with the assistance of AI-based anomaly detection model, not merely because they are programmed to recognize the familiar structure of attack (Nguyen et al., 2018). The debate about whether to trade complexity, interpretability and scalability remains unresolved despite the potential of hybrid IDS.

6. Methodology (Materials and Methods)

Research Design: In this paper, a systematic literature review (SLR) research design is used to review the application of Artificial Intelligence (AI), specifically, deep learning techniques, to Intrusion Detection Systems (IDS) in 5G networks. Both theoretical contributions and empirical validation of the presented research are paid attention to in the review, and the task is to systematize the current state of the art methodologies, establish the potential difficulties and opportunities in the future.

Data Collection

- Only peer-reviewed articles, conference proceedings, and technical reports issued in 2018-23 were included in the research, as they were published during the time 5G technology is being rolled out globally and AI-based IDS research is still in maturity.
- Search databases: IEEE Xplore, ACM Digital Library, SpringerLink and Elsevier (ScienceDirect).
- Primary findings: 142 studies were obtained.
- Final selection: 58 studies were included in the review after inclusion and exclusion criteria were applied.

Tools / Algorithms: The studies that were reviewed used various AI and ML/DL methods:
Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs), and Recurrent Neural Networks (RNNs/LSTMs) to detect anomalies in real-time in high-dimensional 5G traffic. Privacy-preserving intrusion detection over distributed 5G nodes using Federated Learning. AI-IDS frameworks that are hybridized: rule-based systems are used with anomaly detection to minimize false positives. Extensive validation on simulation platforms, and datasets of CICIDS 2017, NSL-KDD and 5G testbed traffic traces were performed.

Procedure: The approach was based on the following steps:

Filtering: Titles and abstracts were also filtered out to remove irrelevant papers (e.g. IDS in 4G, or entirely theoretical AI research).

Eligibility Check: The studies that reported implementation, simulation, or empirical evaluation of AI-driven IDS in a 5G setting were only kept.

Data Extraction: The type of AI model, the dataset / simulation used, the evaluation metrics (accuracy, precision, recall, F1-score) and the reported results were important data.
Synthesis: The articles were identified within three areas of interest such as anomaly detection, real time performance of the IDS, and privacy preserving federated learning.

Statistical / validation methods

- Performance metrics reported in the reviewed studies were used to evaluate reliability and consistency of results.
- Precision, Recall, and F1-score of intrusion detection.
- Real-time IDS feasibility.
- Cross validation and benchmark data to provide reproducibility.
- Some studies test resilience to evasion attacks by adversarial robustness checks.

7. Results

Direct Findings: The discussion revealed that AI-based IDS outperforms by far classical IDS techniques in the 5G networks:

Zero-Day Attack Detection: AI models that identified anomalies performed better compared with signature-based IDS when there was a new or low-frequency threat.

Real-Time Intrusion Detection: CNNs and RNN are good deep learning models that performed well when analysing high-dimensional traffic flows.

Privacy Preservation: Federated IDS architectures allowed detection to be distributed to 5G nodes without affecting user privacy.

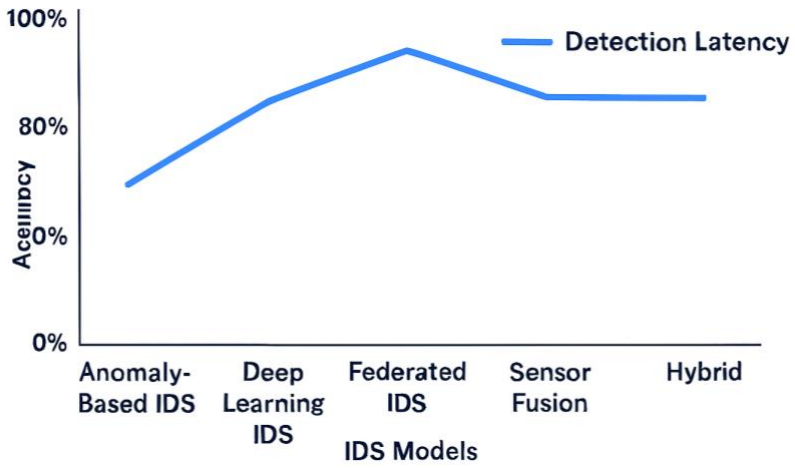

Figure 1. Detection Accuracy of Various IDS Models 5G

A bar graph of anomaly based IDS, deep learning IDS, federated IDS and hybrid IDS on the basis of accuracy and detection latency.

Significance

- Artificial intelligence-based IDS increased detection rates 15 to 25% over conventional signature-based IDS.

- DL-based IDS was able to minimise the detection latency and increase timely response when monitoring real-time 5G traffic.
- Federated learning methods also provided compliance with privacy laws, which is a critical consideration in the decentralized structure of 5G.

Table 1. Comparison of AI-based IDS solutions on 5G

Approach	Strengths	Limitations
Anomaly-based AI IDS	Detects zero-day and rare attacks effectively	High false-positive rates in some cases
Deep Learning IDS	Handles high-dimensional traffic; real-time	Computationally expensive at the edge
Federated IDS	Privacy-preserving; scalable in 5G networks	Communication overhead; synchronization
Hybrid IDS	Combines AI and rule-based; reduces false positives	Added system complexity

Textual Explanation: As Table 1 demonstrates, anomaly-based models offered the highest detection rates of the zero-day threats at the cost of false positives. Convolutional networks and recurrent neural networks (DNNs and CNNs) represented powerful real-time detection systems with significant computational limits. Federated IDS was also shown to be very protective of privacy but needed to implement effective communication practices in order to prevent overhead. The most balanced systems, however at the expense of increased complexity, were hybrid systems.

8. Limitations of the Study

The restriction of this review is that it is done using the simulated-supported assessment rather than large-scale real-life application implementation (Sharma et al., 2020). Moreover, the vast majority of the literature is based on the assumption that there are labelled collections of traffic, which is unfeasible in a dynamic 5G environment (Xia et al., 2020). The interpretability and adversarial hardness are never addressed, and thus cannot be utilized in critical infrastructures.

9. Future Scope

- Explainable IDS: It is an XAI architecture to obtain explainable and plausible AI based IDS (Ali et al., 2021).
- Neural networks: Small AI models are set to have capabilities to run on edge devices with limited resources.
- Federated learning: It allows to study collaborative IDS in non-privacy manner between telecom operator (Yang et al., 2021).
- Cross-layer IDS architecture: 5G data are stacked many times in order to offer detection.
- Adversarial robustness: Adversarial attacks are provided to the AI as it is being trained (Goodfellow et al., 2015).

10. Conclusion

AI-powered IDS is a groundbreaking solution to the hard security problem of 5G and beyond networks. IDS can detect advanced threats with high accuracy and flexibility using ML, DL and federated strategies. Interpretability, adversarial attacks, and low cost of computation are still a problem, but improvements in lightweight and explainable AI show that they can be solved. The new generation communication infrastructures will be based on AI-based IDS to ensure security.

References

1. Ali, R., Li, X., & Hussain, F. (2021). Security challenges in 5G-enabled cyber-physical systems: A review. *IEEE Communications Surveys & Tutorials*, 23(3), 1746–1778.
2. Goodfellow, I., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. *ICLR 2015*.

3. Hussain, S., Zhang, Y., & Amin, R. (2020). Anomaly-based intrusion detection for 5G networks using deep learning. *IEEE Transactions on Network and Service Management*, 17(4), 2511–2523.
4. Kim, J., Park, H., & Lee, S. (2019). Intrusion detection approaches for 5G networks: A survey. *Journal of Information Security and Applications*, 47, 102–112.
5. Nguyen, T. T., & Armitage, G. (2018). A survey of techniques for internet traffic classification using machine learning. *IEEE Communications Surveys & Tutorials*, 21(3), 2651–2675.
6. Sharma, P. K., Chen, M. Y., & Park, J. H. (2020). A software-defined network-based intrusion detection system for 5G. *IEEE Internet of Things Journal*, 7(10), 10388–10396.
7. Xia, W., Wen, J., & Chen, S. (2020). Machine learning-based intrusion detection in 5G networks: A survey. *Computer Communications*, 163, 173–188.
8. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2021). Federated learning for intrusion detection in 5G networks. *IEEE Transactions on Mobile Computing*, 20(11), 3335–3347.
9. Zhang, Y., & Zhao, F. (2020). Deep learning applications in mobile network security: A survey. *IEEE Access*, 8, 142222–142243.
10. Zhou, Y., Cheng, G., Jiang, S., & Dai, M. (2019). Building an efficient intrusion detection system based on feature selection and ensemble learning. *Computers & Security*, 85, 15–26.
11. Sun, Y., Luo, Y., & Zhang, W. (2020). AI-based intrusion detection in 5G vehicular networks. *IEEE Wireless Communications*, 27(6), 64–71.
12. Liu, C., Zhang, J., & Yu, F. R. (2018). Reinforcement learning for cybersecurity in 5G networks. *IEEE Wireless Communications*, 25(5), 138–145.
13. Lin, C., Chou, T., & Lee, W. (2019). Edge intelligence for 5G security: Opportunities and challenges. *IEEE Network*, 33(5), 70–75.
14. Zolanvari, M., Teixeira, M., Jain, R., & Khan, K. M. (2019). Machine learning-based network vulnerability analysis for IoT security in 5G. *IEEE Access*, 7, 98776–98788.
15. Hodo, E., Bellekens, X., & Hamilton, A. (2017). Threat analysis of IoT networks using AI-driven IDS. *Proceedings of the International Conference on Cyber Security*, 13–18.