# Chapter 8
# A Survey on 5G Wireless Network Intrusion Detection Systems Using Machine Learning Techniques

**Michael Chai Chon Yun**
https://orcid.org/0009-0004-3256-2902
*Curtin University, Malaysia*

**Sivaraman Eswaran**
https://orcid.org/0000-0003-0858-148X
*Curtin University, Malaysia*

## ABSTRACT

*This survey explores the landscape of Intrusion Detection Systems (IDS) in 5G wireless networks, with a specific emphasis on those leveraging Machine Learning (ML) techniques. The deployment of 5G is poised to revolutionize telecommunications with unprecedented data rates, reduced latency, and enhanced capacity. However, the advanced infrastructure also brings heightened security challenges, necessitating robust and adaptive security measures. IDS have emerged as a key strategy to counteract these vulnerabilities, particularly those that exploit machine learning for anomaly detection and rapid response. This paper reviews several 5G IDS implementations across different domains, including the 5G Core Network, Internet of Things (IoT), and Smart Grids. Each domain's technical and cybersecurity environment is explored for better context in understanding the different implementations available, which are scrutinised based on ML models used, datasets*

DOI: 10.4018/979-8-3373-0857-9.ch008

*for training and testing, and architecture.*

## INTRODUCTION

Fifth-generation wireless networks, commonly known as 5G, is the latest poster child in telecommunication innovation that introduces new features and exponentially superior performance against its predecessors (Flinders & Smalley, 2024). According to a global economic study by IHS Markit and Omdia (2020), the roll out of 5G is projected to generate 3.8 trillion US dollars' worth of added GDP, and create 22.8 million new jobs in the global value economy. Wang et al. (2021) also points out that the adoption of 5G into industry, agriculture, and infrastructure, can amplify process efficiency, and limit resource utilisation for better sustainability on the long run. With 5G adoption being inevitable, comes the need to ensure its implementation respects security and privacy.

5G infrastructure is a prime target by adversaries due to its hosting of abundant private data and high-value operations (Deloitte, 2020). Moreover, threat actors look forward to leveraging the larger attack landscape and new zero-days that comes with 5G (Cybersecurity and Infrastructure Security Agency (CISA), 2021). Network security solutions are diverse and multifaceted, but this survey shall focus on an industry favourite solution that has proven its effectiveness, the Intrusion Detection System (IDS). This survey looks into different IDS implementations in 5G networks across multiple areas, with an additional emphasis on 5G-IDS that utilise machine learning (ML) techniques. As more modern security solutions embrace machine learning for better efficiency, and effectiveness against zero-days and unknown attacks, which often evade legacy signature-based IDS (Ni, 2023).

This chapter also looks into the design and engineering of 5G, how it is implemented into different areas, its unique security vulnerabilities, and the different IDS solutions to address them. IDS implementations into the 5G Core, 5G Internet-of-Things (IoT), and 5G Smart Grids, are observed and compared. From its findings, there is an abundance of 5G IDS implementations that address these different application areas and possess fine performance. However, a gap found within the survey is the lack of privacy preserving features in these 5G IDS solutions, especially when the ML models employed collect and aggregate private network data for further training. Albeit this, some IDS implementations in 5G IoT and 5G Smart Grids manage to successfully integrate Federated Learning (FL) as a ML model mechanism to keep private network data local and not shared with other ML models in training. But rather ironically, there's a lack of FL utilisation, or any other privacy preserving features for that matter, in IDS for 5G Core, when 5G Core is the backbone of public 5G infrastructure that hosts the most private data and mission critical operations.