

Chapter 4

Network Intrusion Detection to Mitigate Jamming and Spoofing Attacks Using Federated Learning: A Comprehensive Survey

Tayyab Rehman

Air University, Pakistan

Noshina Tariq


 <https://orcid.org/0000-0002-9754-253X>

Air University, Pakistan

Muhammad Ashraf

Air University, Pakistan

Mamoona Humayun

 <https://orcid.org/0000-0001-6339-2257>

Jouf University, Saudi Arabia

ABSTRACT

Network intrusions through jamming and spoofing attacks have become increasingly prevalent. The ability to detect such threats at early stages is necessary for preventing a successful attack from occurring. This survey chapter thoroughly overviews the demand for sophisticated intrusion detection systems (IDS) and how cutting-edge techniques, like federated learning-enabled IDS, can reduce privacy risks and protect confidential data during intrusion detection. It explores numerous mitigation strategies used to defend against these assaults, highlighting the significance of early detection and avoidance. The chapter comprehensively analyzes spoofing and jamming attacks, explores mitigation techniques, highlights challenges in implementing federated learning-based IDS, and compares diverse strategies for their real-world effects on network security. Lastly, it presents an unbiased evaluation of contemporary IDS techniques, assessing their advantages, disadvantages, and overall effect on network security while also discussing future challenges and prospects for academia and industry.

DOI: 10.4018/978-1-6684-7625-3.ch004

INTRODUCTION

The growing prevalence of jamming and spoofing attacks in wireless networks is a cause for concern. The need to develop effective countermeasures has become even more urgent in recent years. Network Intrusion Detection (NID) can be a critical component for protecting against these attacks by detecting malicious activity or events within the network environment (Chaabouni, 2019). However, NID systems have limited effectiveness when faced with complex attack scenarios such as those arising from asymmetric links between multiple Access Points (APs) (Basati, 2023). To address this limitation, novel techniques based on Federated Learning (FL) which utilize data collected from APs across different locations, should be explored. This paper presents an overview of state-of-the-art methods related to NID using federated learning approaches and discusses future directions that researchers should explore in order to create highly secure and resilient network environments against jamming and spoofing attacks (Han, 2022).

Therefore, mitigation goals focus on seeking structured solutions, including security methods such as cryptography-based protection techniques. It may rely on encryption processes explicitly designed to deter Cryptographic Suite Assessment (CSA) against these common types of cyberattacks mentioned above. Detecting suspicious messages before they take proper form within protocols so establishing control mechanisms is vital for anti-jam/spoof detection engines. In addition, isolating any physical attackers by designing efficient countermeasures to avoid existing environmental noise contributed during vulnerable period's demands solutions. Moreover, applying appropriate access controls allows only trusted entities to interact with targeted services or resources and blocks user's authentication by attempting open connections from alleged compromised location(s) (Khan K. M., 2020), (Alloghani, 2019).

Therefore, reducing threats from jamming and spoofing is essential due to their capacity to stop reliable service delivery, as well as financial losses related to assets being exposed often overlooked. It may lead to potentially catastrophic results if no preventive action is taken (Vaishnavi, 2021). Implementation in advance leverages appropriate defences and helps in addressing vulnerabilities that reoccur in the future. It may ultimately harm organizations and raise consequences. Safeguarding also gives the most significant level of assurance for the needed infrastructures' Successful configuration and other benefits, including satisfaction to all parties engaged in the transactions, specified trajectory target operates safely, expects to fulfil compliance rules (YAMAN, 2023). Customer esteem and loyalty, additional growth for the organization, and a positive side scale (Yu, 2022). Multiple difficulties in the execution need good collaboration to protect the investment (Liu, 2022). This survey paper aims to provide a comprehensive review of the research on using federated learning to develop network intrusion detection systems that can mitigate jamming and spoofing attacks (Yin, 2020). The scope of the paper will include an overview of the current state-of-the-art intrusion detection systems, the challenges associated with jamming and spoofing attacks, and the application of federated learning in intrusion detection systems (Kulkarni, 2020), (Belenguer, A review of federated learning in intrusion detection systems for iot. arXiv preprint arXiv:2204.12443., 2022).

In addition to this, the article investigates numerous federated learning algorithms that are used for data manipulation, the protection of privacy, jamming, and spoofing attacks. It also highlights the strengths and weaknesses of federated learning methods, specifically how they are used in network intrusion detection systems (Belenguer, 2022). This survey paper aims to connect intrusion detection systems and federated learning research by comprehensively investigating how federated learning can be used to make intrusion detection systems that protect against jamming and spoofing attacks. The survey paper will also help determine the problems and limits of using federated learning in network intrusion

22 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/network-intrusion-detection-to-mitigate-jamming-and-spoofing-attacks-using-federated-leading/339248

Related Content

The Impact of Data Strategy and Emerging Technologies on Business Performance

Subbarao Pothineni (2023). *International Journal of Business Strategy and Automation* (pp. 1-19).
www.irma-international.org/article/the-impact-of-data-strategy-and-emerging-technologies-on-business-performance/334022

Marketing of Private Labels: Strategies and Initiatives

Pratap Chandra Mandal (2021). *International Journal of Business Strategy and Automation* (pp. 70-81).
www.irma-international.org/article/marketing-of-private-labels/269497

Digital Twin-Driven Condition-Based Maintenance

Adolfo Crespo del Castillo, Marco Macchiand Laura Cattaneo (2022). *Cases on Optimizing the Asset Management Process* (pp. 109-136).
www.irma-international.org/chapter/digital-twin-driven-condition-based-maintenance/289742

Material Handling and Product Optimality of an Educational Institution Bakery Using Integer Programming

Adedugba Adebayo, Ogunnaike Olaleke, Kingsley Adeyemoand Busola Kehinde (2021). *International Journal of Business Strategy and Automation* (pp. 53-61).
www.irma-international.org/article/material-handling-and-product-optimality-of-an-educational-institution-bakery-using-integer-programming/282521

Airline Effective Green Operations Strategy Patterns: Regional Level Analysis

(2020). *Airline Green Operations Strategies: Emerging Research and Opportunities* (pp. 172-189).
www.irma-international.org/chapter/airline-effective-green-operations-strategy-patterns/256781