© JAN 2026 | IRE Journals | Volume 9 Issue 7 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I7-1713355

Towards Zero Touch Networks: Cross-Layer Automated Security Solutions For 6G Wireless Network

PRIYA B A[1], SAHANA S[2]
[1, 2]*Student, Artificial Intelligence and Data Science, SJC Institute of Technology, Chickballapur, Karnataka, India*

Abstract- ***The evolution toward 6G wireless networks introduces unprecedented demands for ultra-low latency, high data rates, and large-scale device connectivity. To meet these challenges, Zero- Touch Networks (ZTNs) powered by Artificial Intelligence (AI) and Machine Learning (ML) are envisioned to automate network operations with minimal human intervention. However, this automation raises significant cybersecurity concerns due to the dynamic nature and complexity of 6G environments. The prevailing cyber defense mechanisms, which often rely on static configurations, human-dependent interventions, and handcrafted detection rules, are inherently inadequate for the dynamic and decentralized architecture of 6G.***

I. INTRODUCTION

The transition from 1G to 5G has drastically transformed mobile communication, and 6G is expected to enhance this further with ultra-low latency, high data rates, and automation. A key enabler for 6G is Zero-Touch Network (ZTN), which aims for fully autonomous network operations using AI/ML. However, ZTNs also increase vulnerability to cyber threats. Current AI/ML solutions for cybersecurity are labor-intensive and struggle with model drift and adaptability. It proposes a comprehensive AutoML-based framework for autonomous cybersecurity, targeting both PLA and CLIDS for robust protection in 6G networks. The rapid advancement of wireless communication technologies has ushered in a new era of hyper-connectivity, with 6G networks on the horizon promising transformative capabilities that extend far beyond the scope of 5G. However, this leap in technological prowess introduces profound challenges—chief among them, the issue of cybersecurity in increasingly autonomous, decentralized, and intelligent network infrastructures. The complexity, scale, and heterogeneity of 6G render traditional security mechanisms, such as static rule-based firewalls, cryptographic protocols, and manual configuration strategies, largely obsolete. Against this backdrop, the concept of Zero-Touch Networks (ZTNs) emerges as both a necessity and a solution. ZTNs, built on the foundational principles of end-to-end automation, AI-driven orchestration, and dynamic resource management, seek to minimize human intervention by enabling networks to configure, secure, and optimize themselves autonomously (1).

II. LITERATURE REVIEW

- M. Liyanage et al - ”A survey on Zero touch network and Service Management (ZSM) for 5G and beyond networks,” Jul. 2022.

As the proliferation of smart Internet-of-Things (IoT) devices and the demand for innovative business services escalate, traditional Network Management and Orchestration (MANO) approaches are increasingly inadequate. The ZSM concept emerges as a solution to this challenge, aiming to automate network and service management to enhance efficiency, scalability, and performance visibility [2] .

Advantages:

- Full Lifecycle Automation: Automates the entire service lifecycle with minimal human intervention.
- Cross-domain Data Handling: Enables seamless sharing and processing of management data , supporting scalability and real-time operations.

Disadvantages:

- Cross-domain Complexity: Coordinating and managing services across different domains is complex and can lead to integration challenges.
- Security & Privacy Concerns: Sharing data and resources across domains introduces risks to data integrity, confidentiality, and compliance.

➢ J. Gallego-Madrid, R. Sanchez-Iborra, P. M. Ruiz, and A. F. Skarmeta -"Machine learning-based zero-touch network and service management: a survey," Apr. 2022.

This delves into the state-of-the-art applications of ML in enhancing ZSM performance. It examines various ML techniques employed in different aspects of ZSM, including multi-tenancy management, traffic monitoring, and architecture coordination. The authors also explore related standardization activities and international research efforts aligned with ZSM, highlighting the rapid growth and adoption of this paradigm[3].

Advantages:

- High Detection Accuracy: Achieves 99.8% accuracy using deep learning on the CICIDS-2018 dataset, demonstrating strong performance in identifying cyber threats.
- Zero-Touch Automation: Enables autonomous intrusion detection in smart cities without human intervention, aligning with the goals of fully automated network security.

Disadvantages:

- High Computational Demands: Requires powerful hardware (e.g., GPUs) and significant resources for model training and real-time operation.
- Limited Generalization: Performance is evaluated on a specific dataset; real-world or unseen scenarios may reduce effectiveness without further validation.

III. OBJECTIVES

Implement automated feature engineering, model selection, and hyper parameter tuning and address model drift using adaptive online learning techniques (1).

IV. METHODOLOGY

Data Collection & Preprocessing - Collect real-world cybersecurity datasets (RF fingerprinting and CICIDS2017) (2).

V. RESULTS

The confusion matrix visually represents how accurately the intrusion detection model classified benign and malicious traffic. It displays the distribution of True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN), allowing a clear understanding of classification performance. A high number of TP and TN indicates that the model correctly identifies most legitimate and attack-related patterns (1).

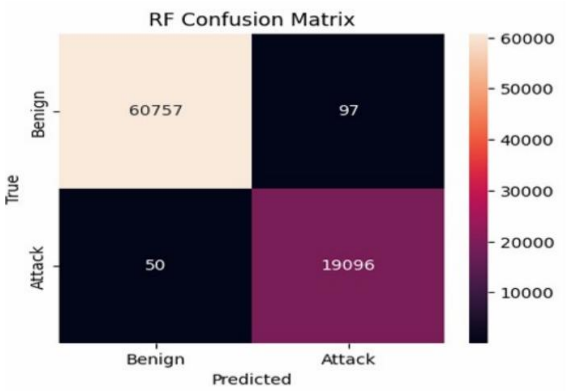

Fig 1: Confusion Matrix

VI. ANALYSIS

The proposed online AutoML framework ad dresses key deployment challenges, including computational demands, cost-effectiveness, adaptability, and operational con tinuity. Its design makes it a practical and scalable solution for integrating AI/ML into next-generation networks while ensuring network performance and security (3).

VII. LIMITATIONS

Limited Evaluation on Real-World 6G Networks

- Experiments are performed on public datasets (RF fingerprinting, CICIDS2017).
- Actual 6G network conditions may show unforeseen challenges, such as more complex attack patterns (1).

VIII. CONCLUSION

The shift toward fully autonomous 6G networks marks a major transformation in how modern communication

systems are designed, managed, and secured. As network environments become more heterogeneous, highly dynamic, and densely interconnected, traditional security mechanisms prove insufficient in ensuring real-time protection and operational reliability. This work addressed these limitations by developing an automated cybersecurity framework combining Physical Layer Authentication (PLA), Cross-Layer Intrusion Detection Systems (CLIDS), and online AutoML-driven security intelligence (2).

REFERENCES

Journal Papers:

[1] Li Yang, Member, IEEE, Shimaa Naser, Member, IEEE, Abdallah Shami, Fellow, IEEE, Sami Muhaidat, Senior Member : “Towards Zero Touch Networks: Cross-Layer Automated Security Solutions for 6G Wireless Networks”, , IEEE, Lyndon Ong, Member, IEEE, and M´ erouane Debbah, Fellow, IEEE, JAN. 2025.

[2] M. Liyanage et al., ”A survey on Zero touch network and Service Management (ZSM) for 5G and beyond networks,” J. Netw. Comput. Appl., vol. 203, p. 103362, Jul. 2022.

[3] J. Gallego-Madrid, R. Sanchez-Iborra, P. M. Ruiz, and A. F. Skarmeta, “Machine learning-based zero-touch network and service management: a survey,” Digit. Commun. Networks, vol. 8, no. 2, pp. 105–123, Apr. 2022.