A ZSM-Based Security Framework for Real-Time Traffic Analysis in Local 5G networks

Mahnsuk Yoon
ICT Device Research Center Gumi
Electronics & Information Technology
Research Institute Gumi, Korea
yms@geri.re.kr

Taeuk Park
ICT Device Research Center Gumi
Electronics & Information Technology
Research Institute Gumi, Korea
ptu @geri.re.kr

Jaeuk Kwon
ICT Device Research Center Gumi
Electronics & Information Technology
Research Institute Gumi, Korea
kwonjuk@geri.re.kr

Yong-An Jung
ICT Device Research Center Gumi
Electronics & Information Technology
Research Institute Gumi, Korea
yajung@geri.re.kr

Sang-Bong Byun
ICT Device Research Center Gumi
Electronics & Information Technology
Research Institute Gumi, Korea
sbbyun@geri.re.kr

Sung-Hune Lee
ICT Device Research Center Gumi
Electronics & Information Technology
Research Institute Gumi, Korea
leesh@geri.re.kr

***Abstract*— As Local 5G networks gain traction in vertical industries such as smart manufacturing, autonomous driving, and digital healthcare, the demand for robust security and reliability has become paramount due to the mission-critical nature of these services. However, the operational environments of such networks often lack the specialized infrastructure and skilled personnel found in traditional mobile network operator (MNO) settings, making them vulnerable to security threats and limiting effective intrusion response. To overcome these limitations, this paper introduces a security framework based on the Zero-touch Service Management (ZSM) paradigm, which enables real-time user-plane traffic analysis and automated threat mitigation with minimal human intervention. The proposed method was implemented and validated in a commercial-grade Local 5G environment, confirming its feasibility and effectiveness for practical deployment in real-world scenarios.**

Keywords*— *Local 5G, Zero-touch Service Management (ZSM), Security Framework, Real-Time Traffic Analysis, Intrusion Detection, Autonomous Network Operation

INTRODUCTION

As the complexity of 5G and next-generation networks continues to grow, the Zero-touch Service Management (ZSM) framework defined by ETSI has emerged as a key architecture for achieving autonomous and secure network operations [1]. ZSM provides an intent-driven automation framework based on closed-loop control, enabling integrated management of diverse network components such as SDN, NFV, MEC, and network slicing. This is particularly critical in mission-critical environments, such as Local 5G deployments, where minimizing manual intervention while ensuring both security and agility is essential.

El Rajab et al. [2] emphasize the intent-based design, end-to-end assurance, and multi-domain integration capabilities of ZSM, demonstrating how closed-loop control is realized in next-generation networks. However, the application of ZSM for session-level security remains at an early stage of exploration.

Research leveraging artificial intelligence (AI) within the ZSM framework is also gaining momentum. Rezazadeh et al. [3] proposed a scalable actor-critic learning approach for autonomous resource control and network slicing optimization. Pradoglou et al. [4] introduced a predictive security response model utilizing both control-plane and user-plane data to enable intelligent threat mitigation. Furthermore, Lira et al. [5] proposed a methodology for translating user intents into executable network configurations using large language models (LLMs), aligning with the autonomous control structure envisioned by ZSM.

Complementary research has further explored enhancing session anomaly detection by combining AutoML techniques with user-plane observability [6], while Sajjad et al. [7] proposed a ZSM-based architectural framework for security management in 3GPP-compliant network slicing. Additionally, lightweight edge-level threat detection mechanisms using AI-enabled observability and eBPF have been studied [8].

These works collectively indicate a clear trend toward AI-driven, intent-aware, closed-loop automation in future network operations. Building on this direction, this study proposes a ZSM-based security framework that integrates session-level behavior monitoring, control-plane telemetry, and AI-powered anomaly detection and response mechanisms.

PROPOSED ZSM-BASED SECURITY FRAMEWORK FOR LOCAL 5G NETWORKS

To enhance the security of Local 5G environments while minimizing operator intervention, this paper proposes a ZSM (Zero-touch Service Management)-based framework for session-level user-plane data traffic analysis and response. The proposed framework is designed around the following three core components:

A. ZSM-Based Closed-Loop Security Analysis Architecture

The framework is built upon the key principles of ZSM, including intent-driven automation and a closed-loop control structure. It enables real-time collection and analysis of user-plane traffic to detect abnormal behaviors. Upon detection, alerts are automatically generated and delivered to network

operators, and if necessary, corresponding response policies can be executed without manual intervention. This architecture aligns with the ZSM paradigm of autonomous and secure network management.

B. Session-Level User-Plane Traffic Analysis Logic

The analysis engine constructs traffic sessions based on Tunnel Endpoint Identifiers (TEIDs) of user equipment and detects anomalies such as abnormal session linkages, TEID duplication, and irregular traffic flows. The framework also identifies session correlations using key fields such as UE IP, IMEI, TEID, and gNB identifiers. Based on this correlation, the system monitors and detects abnormal data traffic at the application level, enabling effective identification and mitigation of potential security threats.

C. Real-Time Operation and Minimal Operator Involvement

The system provides a web-based interface through which users can perform real-time session-level traffic analysis and automatically detect anomalies. All analysis processes and response actions are communicated via real-time messaging, and the results are automatically visualized for immediate review. This end-to-end automation of traffic collection, analysis, and result visualization eliminates the need for manual operator involvement, thereby fulfilling the zero-touch operation requirements defined by the ZSM framework.

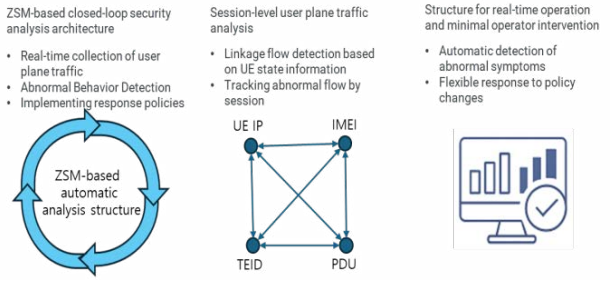

Fig. 1. ZSM-Based Framework for Session-Level Security Analysis and Real-Time Operation in Local 5G Networks

The proposed approach defines an automated security analysis framework leveraging the closed-loop structure of ZSM, with a focus on fine-grained session-level traffic analysis logic and real-time operational mechanisms. Each component is designed with real-time responsiveness and automation at its core, enabling swift and efficient responses to security threats in Local 5G environments. Through this design, the architecture concretely realizes the autonomous network security management envisioned by the ZSM framework in practical deployment scenarios.

IMPLEMENTATION

The proposed framework was tested by interworking it with a commercial Nokia 5G standalone testbed. Session data was collected from the AMF and UPF every 15 minutes to observe traffic flow and session status. In the integrated environment, the anomaly detection engine successfully received and parsed real session data, and response policies were triggered automatically according to defined thresholds. This experiment verified the interworking capability of the framework in terms of log collection, session flow analysis, and basic automated policy execution. Further experiments with large-scale traffic and advanced predictive models are planned as future work.

CONCLUSION

This paper presents a unified ZSM-based architecture for enhancing security and automation in 5G private networks. The proposed framework enables session-level monitoring, anomaly detection, and policy enforcement with minimal human intervention. Future work includes refining real-time data pipelines, integrating reinforcement learning for policy optimization, and extending compatibility with 6G and intent-based network architectures.

ACKNOWLEDGEMENT

This work was partly supported by the Institute of Information & Communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT) (No. RS-2024-00397469, Development of Private 5G Security Technology for Integrated Private 5G and Enterprise Network Security, 100%)

REFERENCES

[1] ETSI, “Zero-touch network and Service Management (ZSM); Reference Architecture,” ETSI GR ZSM 004 V2.1.1, 2022.

[2] M. El Rajab, S. Yang, and A. Shami, “Zero-Touch Networks: Towards Next-Generation Network Automation,” arXiv preprint arXiv:2312.04159, 2023.

[3] A. Rezazadeh, M. F. Bari, and R. Boutaba, “Zero-touch Continuous Network Slicing Control via Scalable Actor-Critic Learning,” arXiv preprint arXiv:2101.06654, 2021.

[4] N. Pradoglou-Grammatikis, P. Sarigiannidis, et al., “Trustworthy Analytics in ETSI ZSM: A 5G Security Case Study,” ResearchGate preprint, 2024.

[5] I. Lira, P. Bosch, and A. Pujol, “Large Language Models for Zero Touch Network Configuration Management,” arXiv preprint arXiv:2408.13298, 2024.

[6] M. El Rajab, S. Yang, and A. Shami, “Machine Learning-Based Zero-Touch Network and Service Management: A Survey,” ResearchGate, 2023.

[7] S. Sajjad, A. Al-Dulaimi, and A. Anpalagan, “ZSM-based Management and Orchestration of 3GPP Network Slicing: An Architectural Framework,” arXiv preprint arXiv:2203.12775, 2022.

[8] Anonymous, “AI-Enabled Observability: Leveraging Emerging Networks for Secure, Resilient, and Adaptive Networks,” *International Journal of Innovative Research in Science and Society (IJIRSS)*, vol. 5, no. 3, 2025.J. G. Herrera, J. F. Botero, Resource allocation in NFV: A comprehensive survey, IEEE Transactions on Network and Service Management 13 (3) (2016) 518-532.