Enhanced Security Architecture for Direct Interworking between Commercial 5G and Defense Networks*

Jisoo Shin, Yongyoon Shin, Hyunjin Kim and Jonggeun Park†
ETRI, Daejeon, KOREA
{jshin, uni2u, be.successor, queue}@etri.re.kr

Abstract

5G mobile communication technology is essential for modernizing the military's communications infrastructure. In order for the national defense network to support real-time, nationwide communications, it should be designed to directly interconnect with commercial networks, accompanied by the implementation of an optimized information security system. We propose a reinforced security architecture for this environment, where commercial 5G and defense networks are directly interconnected.

1 Introduction

Our military is making various efforts to modernize its communications infrastructure. Since the defense network requires an extremely high level of security, the current indirect communication is difficult to ensure real-time performance. Meanwhile, due to the structural and service environment changes brought by 5G, new potential threats are emerging in addition to existing threats in 4G [1].

5G-ACIA proposed four deployment models for private 5G networks [2]. From the military's perspective, the shared RAN model is the most suitable option for achieving nationwide coverage at relatively low deployment costs while maintaining a high level of security.

2 Commercial 5G-Defense Network Interworking Architecture

The proposed interworking security structure includes a non-secure commercial network within end-to-end connections. Therefore, to ensure a secure direct interconnection, it can be divided into three parts. First, Device Security Technology consists of hardware or software KCMVP (Korea Cryptographic Module Validation Program) encryption module and Mobile Device Management technology. Data encrypted through the encryption module provides end-to-end protection up to the VPN G/W using encryption algorithms mandated by the military.

* Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-78, December 16-18, 2025, Sapporo, Japan.
† Corresponding author

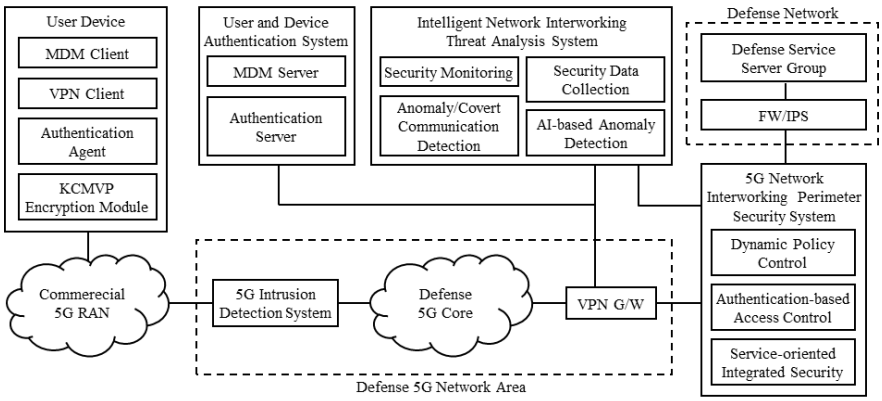

Figure 1: Enhanced security structure for direct interworking between commercial 5G and defense networks

Second, 5G Network Interworking Security Technology consists of 5G Intrusion Detection System and the 5G Network Interworking Perimeter Security System. The former, at the front end of the 5G core, protects the core from well-known attacks targeting signaling traffic (N2 interface) and data traffic (N3/N9). The latter, based on cloud-native, dynamically provides user-authorized access control, optimized firewalls for each converged service, web firewalls, and IPS/IDS (N6).

Finaly, Intelligent Network Interworking Security Technology enhances security intelligence by analyzing correlations among traffic, data, and security events generated through the interconnection with commercial 5G networks. This enables the system to respond to unknown and critical attacks using AI-based techniques. The analysis results are shared with the 5G Network Interworking Perimeter Security System, enabling efficient response to new network threats.

3 Conclusion

We proposed a security architecture capable of dynamically responding to various cyberattacks in an environment where commercial and defense networks are directly interconnected. We expect that the proposed structure will safely support our military's diverse future defense services.

4 Acknowledgments

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (Ministry of National Defense) (RS-2022-11220701, Development of Security Technology for Interworking between M-BcN and 5G Commercial Network).

References

[1] Jong-Geun Park, “Trends and Security Technologies in 5G Private Networks,” *Journal of the Korean Institute of Communications and Information Sciences*, Vol. 40, No. 9, pp. 21-29, 2023.

[2] 5G Non-Public Networks for Industrial Scenarios, 5G-ACIA, 2019, https://5g-acia.org/wp_5g_npn_2019_01