Provision of Defense 5G Mobile Communication Services Using Commercial Radio Access Network and Wireless Backhaul

Jin-Kyu Choi†, HyunSoon Nam†, Jongkuk Lee†, HeaSook Park‡
Defense ICT Convergence Research Section†
Defense & Safety Convergence Research Division‡
Electronics and Telecommunications Research Institute (ETRI)
{jkchoi, namhs, raphael, parkhs}@etri.re.kr

***Abstract*—If the military and related government agencies can receive defense information and communication services using a 5G mobile network, they can transmit and process necessary information more quickly and securely. This enables the military to collect situational information in real-time and share it with commanders, which can support rapid decision-making. To achieve this, using a commercial 5G cell site is more efficient than installing additional dedicated military base stations, as it can reduce the cost and manpower required for installation and operation. However, secure authentication and strong security measures are necessary to prevent disruption of enemy communication networks and information theft. Wireless backhauls are also needed to support communication in areas where commercial base stations are not installed. In this case, a wider variety of wireless access scenarios need to be diagnosed for failures, and the quality of communication services need to be measured for optimizing network performance. This paper explains the concept of providing defense information and communication services using commercial 5G base stations and mobile wireless backhauls. Additionally, it describes the specific technologies required to achieve this goal.**

***Index Terms*—Defense 5G, Defense network, 5G core network**

I. Introduction

The defense ministries of major world countries are striving to establish a 5G-based military mobile infrastructure, not only for military operations but also for education and training, as well as for the living quarters of soldiers [1]–[3]. Smart devices and various sensors collected from operational areas will be processed and transmitted in real-time to support decision-making by commanders, while 5G mobile communication will be employed in border operations to monitor civilian fishing boats and illegal fishing vessels in coastal areas [4]. The education and training of soldiers to configure the command and control system using tactical communication equipment, powered up in the military and the soldiers' living quarters, will also be essential tools. However, building a large-scale military-only cell site to establish a military 5G mobile network is inefficient in terms of installation and operation costs. Therefore, significant cost savings can be achieved by utilizing commercial 5G radio access network (RAN) with security technology. Mobile edge computing technology and mobile backhaul will enhance the survivability of military 5G networks in operational areas where commercial base stations have not been installed or have been destroyed by the enemy [5]–[10]. For a better understanding, the rest of this paper is organized as follows: Section 2 describes the network scenarios of the defense 5G mobile services, and Section 3 discusses the technical challenges of utilizing commercial and military-only radio access networks simultaneously. Section 4 introduces the system architecture for measuring the overall network's failure or quality, and finally, Section 5 presents a brief summary of the conclusion.

II. Network Scenarios

There are various network scenarios of the military for accessing defense networks using commercial smartphones or legacy devices such as drones, robots as shown in figure 1 and table 1.

A. Secure access through 5G commercial network

Soldiers are equipped with security modules on their personal smartphones and access the Military Mobile Core Network (M-MCN) through 5G commercial cell sites, primarily utilizing the already installed 5G commercial network in urban areas to save additional base station installation and operation costs. However, various security measures are necessary to prevent military information from remaining on commercial smartphones and base stations.

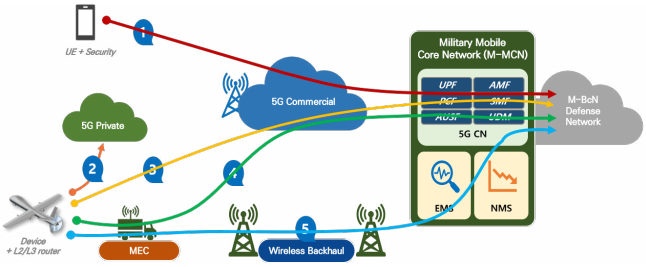

Fig. 1. Network concepts for the defense 5G mobile services.

TABLE I
NETWORK SCENARIOS OF THE DEFENSE 5G MOBILE SERVICES.

Access type	User equipment	Network scenarios
Commercial	Commercial phone	gNB + M-MCN + DN
	Legacy device	gNB + M-MCN + DN
		MEC + gNB + M-MCN + DN
Private	Legacy device	MEC + W.B + M-MCN + DN
		5GPN

B. Access to military dedicated 5G network

The military's dedicated 5G network uses separate frequencies for access, so dedicated mobile routers and security technologies are applied.

C. Deployment of 5G networks for tactical assets using commercial RAN

To transmit operational video data produced by tactical assets such as robots, drones, sensors, cameras, AR/VR devices, and autonomous vehicles over commercial 5G networks, multiple levels of authentication and security policies are essential.

D. Deployment of mobile edge cloud

Mobile MEC (Multi-access Edge Computing) can collect data from various types of devices in military operation areas and perform functions such as immediate AI-based automation, video data analysis, and remote robot control on site.

E. Expanding communication availability through wireless backhaul.

In operation areas where commercial 5G RAN access is not possible or cell sites are destroyed by the enemy, direct access to the M-MCN is made via wireless backhaul.

III. TECHNICAL CHALLENGES

A. Cryptographic Module for UE

To secure the 5G Radio Access Network, network security settings are configured on wireless devices, and encryption modules for RAN end-to-end segment encryption are installed on commercial smartphones. Also, additional research is needed to reduce the data rate reduction by a factor of several due to the encryption module.

B. Access to the defense core network from commercial 5G RAN

To protect military information from commercial core networks, a GTP-U (GPRS Tunneling Protocol) tunnel must be established from the commercial 5G gNB to the M-MCN.

C. User authentication for accessing defense network

To allow access to military networks in conjunction with user authentication on commercial 5G networks, additional authentication is required for users and user terminals.

D. Trusted interoperation between mobile MEC and defense networks

Mobile MECs for securing communication coverage and establishing edge cloud environment for mission requirements in operational areas should be capable of collecting, storing, sharing data on site, and securely connecting to defense networks.

E. Network fault detection and quality measurement

Since more network elements and access points are added compared to commercial 5G networks, it is necessary to measure failure detection and network quality for each section and optimize user performance.

IV. NETWORK QUALITY MEASUREMENTS

A. Fault detection of radio access network

Since the operator of the 5G commercial network and the operator of the defense network are different, and various application servers used by the users are managed separately, monitoring is required to identify where a problem occurred, and to measure the quality of the network as shown in figure 2.

B. Wired network quality measurement

When the UPF (User Plane Function) for military terminals is processed in M-MCN, it is transmitted to each military application server via M-BcN (Military-Broadband Convergence Network). The quality measurement results for wired networks are reported to each network operator, enabling maintenance.

C. Network access point statistical analysis

In network components such as M-MEC, M-MCN, and M-BCN, information on UPF statistical characteristics is collected and analyzed.

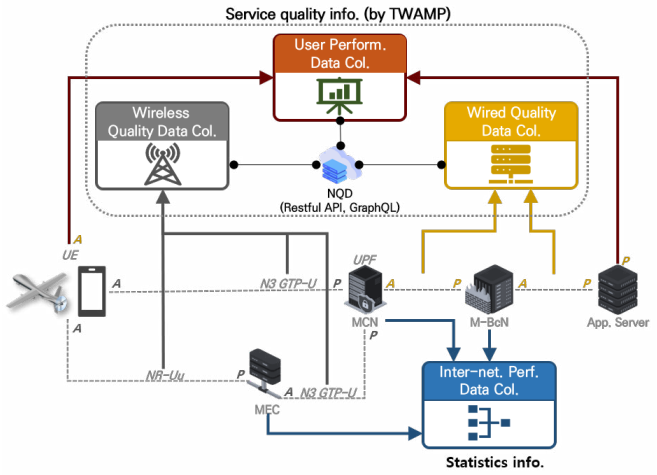

Fig. 2. Data collection for network quality measurement.

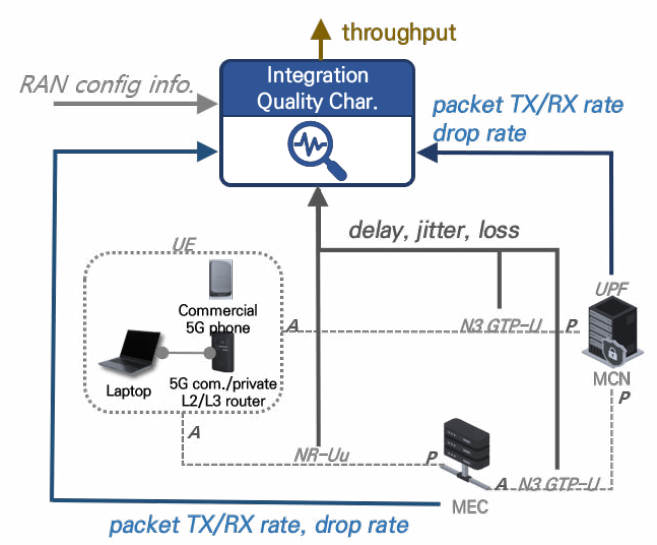

Fig. 3. User performance prediction using network statistics information.

D. User performance monitoring

Since the performance of the application used by the user is the result of adding up the end-to-end performance of the entire network, monitoring the user's performance enables monitoring the quality of the military 5G mobile communication service. Furthermore, performance monitoring of the radio access network can be carried out based on the collected statistical information, as shown in figure 3.

the network scenarios of the defense 5G mobile services, and section 3 discusses the technical challenges of utilizing commercial and military-only radio access networks simultaneously. Section 4 introduces the system architecture for measuring the overall network's failure or quality,

V. Conclusion

In this paper, we have described network scenarios for providing defense 5G mobile services and discussed the technical challenges of accessing defense networks by utilizing both commercial and military-dedicated radio access networks. In particular, we introduced the structure of a network quality measurement system for ensuring connectivity and survivability of the network and monitoring user performance. When the defense 5G mobile service presented in this paper is fully operationalized, it is expected to increase communication availability for unmanned systems in the future battlefield, thus becoming an important asset for future warfare.

Acknowledgment

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (2022-0-00030, Development of trust inter-networking technology of defense mobile environment for real-time information sharing)

References

[1] M. E. Dempsey and S. Rasmussen, "Eyes of the army–us army roadmap for unmanned aircraft systems 2010–2035," *US Army UAS Center of Excellence, Ft. Rucker, Alabma*, vol. 9, 2010.

[2] U. D. of Defense, "Unmanned systems integrated roadmap: Fy2013–2038," 2013.

[3] K. Fahey and M. Miller, "Unmanned systems integrated roadmap 2017–2042," *Department of Defense*, 2017.

[4] J.-K. Choi, Y.-T. Lee, H. Park, B. Kim, and B.-W. Kim, "Challenges to the development of manned and unmanned combat systems," in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2022, pp. 2362–2364.

[5] S. Nam, "The impact of 5g multi-access edge computing cooperation announcement on the telecom operators' firm value," *ETRI Journal*, vol. 44, no. 4, pp. 588–598, 2022.

[6] H. Lee, G.-M. Um, S. Y. Lim, J. Seo, and M. Gwak, "Real-time multi-gpu-based 8kvr stitching and streaming on 5g mec/cloud environments," *ETRI Journal*, vol. 44, no. 1, pp. 62–72, 2022.

[7] J. Yun, Y. Goh, W. Yoo, and J.-M. Chung, "5g multi-rat urllc and embb dynamic task offloading with mec resource allocation using distributed deep reinforcement learning," *IEEE Internet of Things Journal*, vol. 9, no. 20, pp. 20 733–20 749, 2022.

[8] S. Nath, S. P. Singh, and S. Sengar, "Interference and noise analysis for hybrid fso/rf-based 6g mobile backhaul," *ETRI Journal*, vol. 44, no. 6, pp. 966–976, 2022.

[9] R. A. Kumar and K. Sumit, "Identifying the leaders and main conspirators of the attacks in terrorist networks," *ETRI Journal*, vol. 44, no. 6, pp. 977–990, 2022. [Online]. Available: https://doi.org/10.4218/etrij.2021-0239

[10] A. Sarker, S. Byun, M. Raavi, J. Kim, J. Kim, and S.-Y. Chang, "Dynamic id randomization for user privacy in mobile network," *ETRI Journal*, vol. 44, no. 6, pp. 903–914, 2022.