Zero Trust Black Network Access for Mobile Broadband Mission-Critical Services

1st Boo Geum Jung
Defense ICT Convergence Research Sec.
ETRI
Daejeon, South Korea
bgjung@etri.re.kr

2nd Yoon-Sik Yoo
Defense ICT Convergence Research Sec.
ETRI
Daejeon, South Korea
ys5315@etri.re.kr

3rd Jinhyuk Yim
Defense ICT Convergence Research Sec.
ETRI
Daejeon, South Korea
jhyim@etri.re.kr

4th KangWoon Hong
Defense ICT Convergence Research Sec.
ETRI
Daejeon, South Korea
gwhong@etri.re.kr

5th Jongkuk Lee
Defense ICT Convergence Research Sec.
ETRI
Daejeon, South Korea
raphael@etri.re.kr

6th HeaSook Park
Defense Safety Convergence Div.
ETRI
Daejeon, South Korea
parkhs@etri.re.kr

***Abstract*—Reliable communications are an important part of public missions. Previously, public safety networks used dedicated networks based on narrowband technology. However, there is current interest in leveraging mobile-based BroadBand(BB) technologies. Therefore, in this paper, we discuss technologies named ZTB(Zero Trust Blacknet) that can safely access Mission-Critical(MC) services in broadband mobile-based public safety networks. A mixture of rapidly deployable tactical bubbles and commercial access networks, zero trust zones require rigorous verification before access to MC server zones. First, we made a kind of tactical bubble with Open5GS and srsRAN. Next, mobile communication with commercial mobile devices takes place in this bubble. We also develop the ZTB Manager, Gateway and Agent functions to provide secure access to the MC server based on the Zero Trust Architecture(ZTA) and Single Packet Authorization(SPA) mechanism. ZTB will help increase the reliability of communications over mobile broadband public safety networks.**

***Index Terms*—ZTA, SPA, Open5GS, srsRAN, SDR, MC service, tactical bubble, public safety network**

I. Introduction

Communications networks for public missions are increasingly relying on mobile network technology. Police officers, paramedics, border guards, and fire and rescue personnel will use tactical bubbles that can be quickly deployed with commercial operators' access networks to communicate. The transition from closed, dedicated infrastructure to these open, hybrid architectures will expand the threat surface and expose mission-critical applications and sensitive information to cyber and physical adversaries [1].

Mobile networks provide access control and provide end-to-end encryption protocols for security. However, for mission-critical communications, these basic measures are not sufficient. Connected to commercial networks, accessed from a variety of devices, and interoperating across organizations, potential persistent threats, including insider threats, proliferate. In order to solve these problems, research is being conducted to strengthen access control and security [2] [3].

Existing studies on tactical bubble coverage and performance [4], MC service protection through network slicing [5] [6], and private mobile network construction [7] are in progress. In this paper, we propose a ZTB framework that fundamentally blocks malicious user access through strong management and verification and provides secure access to mission-critical services in the zero trust area.

Following the introduction, Section 2 proposes the ZTB system model, and Section 3 describes the design and implementation of the ZTB framework. Section 4 shows the verification results of the ZTB and concludes in Section 5.

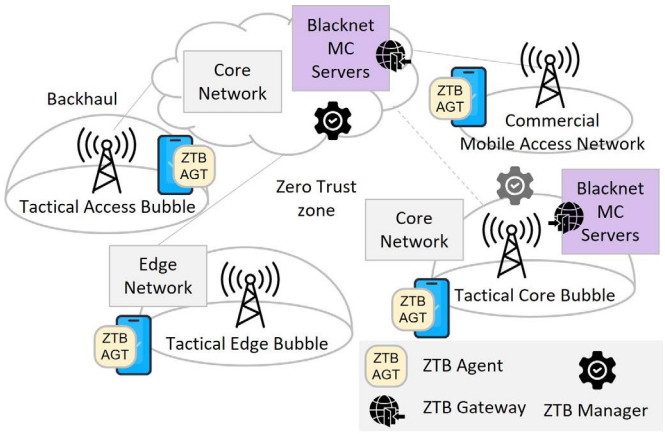

Fig. 1. ZTB Architecture for MC Services on hybrid mobile BB Network.

II. System Model

Section 2 presents the system model in Fig. 1. It consists of three functional blocks ZTB Agent, ZTB Gateway, and ZTB Manager. ZTB Agent is an app installed on mobile devices. The ZTB manager is located in core network and the gateway is connected through the core network from mobile devices. Mission-critical services can only be accessed through

the ZTB gateway. Tactical bubbles and commercial access networks are considered Zero Trust areas.

A. Zero Trust Architecture(ZTA)

Traditionally, cybersecurity is based on a network perimeter that protects internal networks from external threats. However, with the recent development of ICT technology, remote access has become the basis, and the distinction between inside and outside is disappearing. Therefore, adequately securing the network perimeter is not enough to combat emerging cyber threats. ZTA is a concept that allows only users and devices with authenticated identities to access permitted resources through a rigorous validation process [8]. ZTA is one of the most needed technology concepts for accessing mission-critical services in an open mobile network environment.

B. Single Packet Authorization(SPA)

SPA is a way to verify trust before establishing an end-to-end session. When a client wants to communicate with a server, the client first sends a packet containing confidential information to the server. The server will only allow the client to establish a session if the information in this single packet is correct. When the communication path is opened, it performs end-to-end encrypted communication and authenticates the identity [9]. This SPA is one great way to implement ZTA.

III. Design & Implementation

Chapter 3 describes the design and implementation of ZTB. As a testbed environment, the Open5GS system, ZTB Manager, and ZTB Gateway were connected through switches, the MC server was connected to the gateway, and the srsRAN and USRP system was built as a mobile access network as shown in Fig. 2. Load a new USIM and install the ZTB AGT app into the UE.

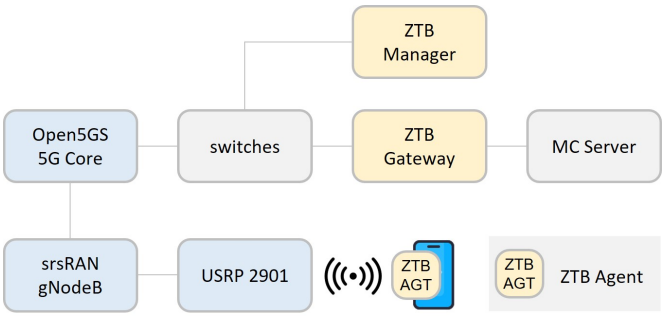

Fig. 2. Design & Implementation Testbed setup.

A. Zero Trust Black Network Agent(ZTB AGT)

ZTB agent generates a SPA message and sends it to the ZTB gateway. SPA messages are transmitted encrypted, protected against replay attacks, and authenticated with HMAC(Hash-based Message Authentication Code) to prevent message tampering and ensure integrity. In addition, the VPN client can be called through the ZTB agent, and the MC service can be called immediately after the VPN connection.

As shown in Fig. 3, a UE equipped with a ZTB agent establishes a 5G connection with 5G Core via USRP and srsRAN gNodeB. After that, a Single Packet Authorization is sent to the ZTB gateway, and the connection to the MC service session is established only after being verified.

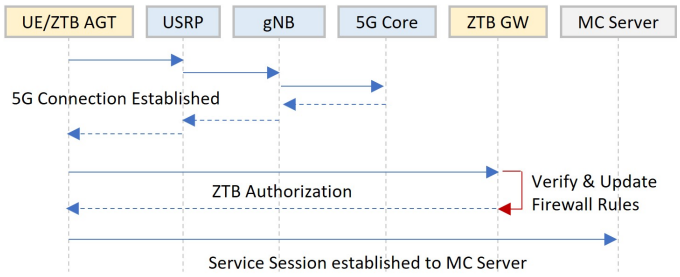

Fig. 3. Sequence Diagram.

B. Zero Trust Black Network Gateway(ZTB Gateway)

By default, the ZTB gateway does not respond to packets other than valid SPA connections. So it is safe from scanning and unauthorized access. It also blocks invalid packets, so DDoS attacks are also blocked. Access attempts that do not start with SPA are judged as abnormal access and help detect security threats.

A valid key, ID, and password for each device are received and set from the ZTB Manager. The policy can then be dynamically changed under the control of the Manager. ZTB Gateway presets VPN between UE and MC server for fast connection (MBS: Make Before SPA). However, since new connection attempt packets and VPN ports are blocked by the firewall, actual access is impossible without passing through the SPA, so it is safe from unauthorized access.

C. Zero Trust Black Network Manager(ZTB Manager)

ZTB manager manages all resources such as users, UEs, gateways, and MC servers. And it plays a role in dynamically controlling the connection between the UEs and the MC services by communicating with the gateway through https.

IV. Verification Results

This chapter describes the verification results of our ZTB framework. We built a private 5G network as a tactical bubble using Open5GS, srsRAN, and USRP. In addition, the USIM of the UE was replaced to access the installed private 5G network. It was confirmed that mobile communication was established and that authorized users and devices were securely connected to the mission-critical server in ZTB framework.

A. Experimental Environment

Table I shows the descriptions for systems equipped with the ZTB framework.

TABLE I
DESCRIPTION OF THE TESTBED

System	Description
UE	Galaxy S22 sysmoUSIM on pysim
SDR	National Instrument(NI)'s USRP2901
5G NR	srsRAN & Open5GS on Ubuntu22.04
ZTB MGR	ZTB Manager SW on Ubuntu 22.04
ZTB GW	ZTB Gateway SW on Ubuntu 22.04
ZTB AGT	ZTB client app on Android 13

B. Test Results

Fig. 4 is a picture of a 5G private network where 5G NR traffic actually flows and connects to the Internet. On the far left is UE, followed by USRP, and 5G Network(RAN and Core). 5G traffic is flowing and YouTube is playing in the COTS UE.

Fig. 4. Actual 5G traffic on UE(through USRP, gNodeB, 5G Core).

A screenshot captured with wireshark of the network interface on the gNodeB system is shown in Fig. 5.

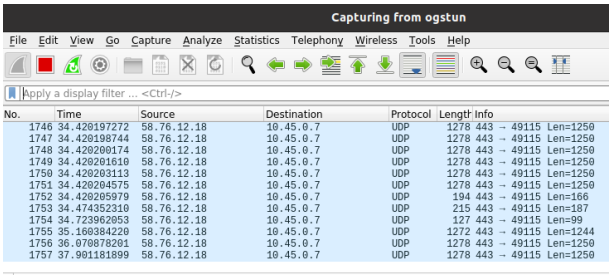

Fig. 5. Traffic Capture on eNodeB(srsenb) through Wireshark.

When ZTB AGT is clicked, the SPA packet is sent to ZTB GW, verified, and then connected to the corresponding service. Fig. 6 shows that the MC service (ZTB APP) is running after ZTB AGT app is clicked.

CONCLUSION

This paper described zero trust black network access technologies for mobile broadband mission-critical services. As the safety net of the future shifts from narrowband to broadband, the threat surface will widen. This paper is meaningful in that it actually builds a 5G core-based tactical bubble and presents the possibility of increasing the reliability of a mobile public safety network by applying a zero trust architecture and a single packet authentication technique. We plan to continue to improve the features and performance of our ZTB framework.

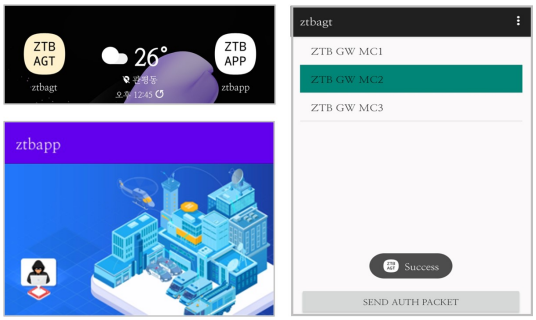

Fig. 6. ZTB AGT execution & Connection to the MC service.

ACKNOWLEDGMENT

This research was supported by the Challengeable Future Defense Technology Research and Development Program through the Agency For Defense Development(ADD) funded by the Defense Acquisition Program Administration(DAPA) in 2022(No.915064201)

REFERENCES

[1] Suomalainen, Jani & Julku, Jukka & Vehkapera, Mikko & Posti, Harri. (2021). Securing Public Safety Communications on Commercial and Tactical 5G Networks: A Survey and Future Research Directions. IEEE Open Journal of the Communications Society. PP. 1-1. 10.1109/OJCOMS.2021.3093529.

[2] Jani Suomalainen, Jukka Julku, Antti Heikkinen, Seppo J. Rantala, Anastasia Yastrebova, Security-driven prioritization for tactical mobile networks, Journal of Information Security and Applications, Volume 67, 2022, 103198, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2022.103198.

[3] S. Wang and R. Ferrús, "On the use of prioritization and network slicing features for mission critical and commercial traffic multiplexing in 5G Radio Access Networks," 2019 IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 2019, pp. 1-6, doi: 10.1109/ISCC47284.2019.8969624.

[4] Heikkilä, Marjo & Koskela, Pekka & Suomalainen, Jani & Lähetkangas, Kalle & Kippola, Tero & Eteläaho, Pentti & Erkkilä, Juha & Pouttu, A.. (2022). Field trial with tactical bubbles for mission critical communications. Transactions on Emerging Telecommunications Technologies. 33. 10.1002/ett.4385.

[5] D. Borsatti et al., "Mission Critical Communications Support With 5G and Network Slicing," in IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 595-607, March 2023, doi: 10.1109/TNSM.2022.3208657.

[6] S. Wang and R. Ferrús, "On the use of prioritization and network slicing features for mission critical and commercial traffic multiplexing in 5G Radio Access Networks," 2019 IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 2019, pp. 1-6, doi: 10.1109/ISCC47284.2019.8969624.

[7] C. S. Choudhari, R. A. Patil and S. Saraf, "Deployment of 5G Core for 5G Private Networks," 2022 International Conference on Industry 4.0 Technology (I4Tech), Pune, India, 2022, pp. 1-6, doi: 10.1109/I4Tech55392.2022.9952900.

[8] Scott Rose, "Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators," 2022 NIST CYBERSECURITY WHITE PAPER, NIST CSWP 20, https://doi.org/10.6028/NIST.CSWP.20.

[9] W. Fang and X. Guan, "Research on iOS Remote Security Access Technology Based on Zero Trust," 2022 IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, 2022, pp. 238-241, doi: 10.1109/ITOEC53115.2022.9734455.