A study on interconnection between local 5G networks and existing networks

Yuji Oishi, Shigenori Hayase, and Masayuki Takase  
Research and Development Group, Hitachi, Ltd.  
1-280 Higashi-Koigakubo, Kokubunji-shi, Tokyo 185-8601, Japan  
yuji.oishi.aw@hitachi.com

Abstract: This paper reports a method for interconnecting local 5G networks and existing networks. Since the two networks are often separated, there is a demand to interconnect the two networks. However, operation gaps such as addressing policy and security policy between the two networks will not allow one to interconnect. To fill the gaps, an interconnection method consists of inter-layer address translation and tunneling in existing networks is proposed and implemented. The evaluation result using an actual local 5G network and an actual corporate intranet revealed that the proposed method works properly.

Keywords: Local 5G networks, Corporate intranet, Interconnection, Address translation, Security

Classification: Network system

References

[1] 5G-ACIA, “5G for connected industries and automation (white paper - second edition),” Feb. 2019.
[2] M. Holdrege and P. Srisuresh, “IP Network Address Translator (NAT) Terminology and Considerations.” RFC 2663, Aug. 1999. https://rfc-editor.org/rfc/rfc2663.txt, DOI:10.17487/RFC2663
[3] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, “IoT security: Ongoing challenges and research opportunities,” 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230–234, 2014. DOI:10.1109/SOCA.2014.58

1 Introduction

Local 5G systems, which enable us to customize mobile networks to specific use-cases, are viewed as a key enabler for smart society such as smart factories[1]. In the “dawn” of local 5G, the local 5G networks are installed for specific use-cases and are isolated from other existing networks such as corporate intranets. While the local 5G system grows from “dawn” to “maturity,” we need to connect the local 5G networks to the existing networks in which existing systems are operated and huge amount of data exist.

However, operational “gaps” prevent us from interconnecting these networks. Here, the “gaps” mean difference in operation policies between these
networks. The gaps include, for example, addressing policy, security policy, application protocol and traffic control. To interconnect these networks, a technique to fill the gaps is required.

2 Operational gaps between local 5G networks and existing networks

The operational gaps arise from the difference in characteristics of the two networks. In this paper, we focus on two fundamental gaps for interconnection shown in Fig. 1: (1) addressing policy and network management layer, and (2) security policy.

We assume Internet of Things (IoT) use-cases. We also assume that a local 5G client system in the local 5G networks of a user equipment (UE) and an IoT terminal directly connected via a local network, and the pair of the UE and the IoT terminal is fixed. The client system is referred as the “terminal” in the following.

![Fig. 1. Operational gaps between local 5G networks and existing networks.](image)

2.1 Gap in addressing policy and network management layer

As two networks are isolated and independent, they have independent addressing authorities which assigns independent addresses in each network. In the worst case, address ranges duplicate and terminals in one network cannot communicate the other network.

An important aspect of addressing policy is network management layers. The intranets are often managed in layer 2, which means the terminals obtain IP addresses by Dynamic Host Configuration Protocol (DHCP) based on their Media Access Control (MAC) addresses. Also, the intranets often adopt MAC address authentication to restrict and manage terminals to connect to the intranet.

On the other hand, the local 5G networks are managed by the core equipment in layer 3, which means the mobile terminals are managed by International Mobile Subscriber Identities (IMSI) and are assigned Internet Protocol (IP) addresses based on IMSIs. As the network management layers
are different, one network cannot manage the other network, thus causes the
duplication of address ranges.

A standard technique called Network Address Translation (NAT)\cite{2} solves
the duplication of address ranges. However, in this case, the DHCP and the
MAC address authentication does not work for the local 5G terminals. This
is because the local 5G terminals do not have the MAC addresses, and the
MAC address of all the packets coming out of the local 5G network is that
of the 5G core.

2.2 Gap in security policy

Assuming IoT use-cases, the local 5G network supports IoT terminals which
have low security capabilities\cite{3}. On the other hand, the intranet often has
strict security policy that the terminals should install anti-virus software
and maintain their security level. Therefore, the local 5G network has lower
security level than the intranet, which is also not acceptable to the intranet
operator. Once the malware invades an IoT terminal in the local 5G network,
then it invades the intranet as well.

3 Proposed method

We propose an interconnection method to fill the two gaps at the boundary
of the two networks. The proposed method consists of two functionalities
called “inter-layer address translation” and “tunneling in intranet.” The
architecture of interconnection is depicted in Fig. 2(a).

![Diagram](image)

(A) Architecture of proposed method

| Mobile address translation table |
|----------------------------------|
| Mobile IP | Intranet IP | Intranet MAC |
| 192.168.1.1 | FF:FF:FF:FF:00:00:01 | 192.168.2.1 |
| 192.168.1.2 | FF:FF:FF:FF:00:00:02 | 192.168.2.2 |

(B) Packets in intranet

| Payload IP | Payload MAC |
| Data | Source: 192.168.1.1 | Destination: 192.168.1.1 |

Intranet address translation table

| Mobile IP | Intranet IP |
| 192.168.7.1 | 192.168.1.1 |
| 192.168.7.2 | 192.168.1.2 |

Fig. 2. Proposed method; (a) Architecture, (b) Behavior of inter-layer address translation.
3.1 Inter-layer address translation
Here we propose an address translation method in a cross-layer manner in-
stead of NAT. Fig. 2(b) shows tables of address translation and the behavior
of inter-layer address translation. There are two tables called “mobile address
translation table (MATT)” and “intranet address translation table (IATT).”

The MATT holds combinations of the IP addresses of the UE in the local
5G network, the MAC address of the IoT terminal, and the IP address for
the intranet. Thus, the MATT translates the IP addresses of the local 5G
network into the MAC addresses of the intranet. The IP address for the
intranet is statically registered or dynamically obtained from DHCP server
in the intranet using the MAC address for the intranet. The IATT holds
combinations of the IP address for the intranet servers and the IP address
for the local 5G. Thus, the IATT translates the IP address of the intranet to
the IP address of the local 5G networks.

Incoming packets from the local 5G network (shown as packet (A)) are
translated their addresses by the MATT and IATT into outgoing packets
to the intranet (shown as packet (B)). The incoming packet has source IP
address of mobile terminal (192.168.1.1) and destination address of the server
(192.168.7.1) for the local 5G.

The MATT translates the source IP address for the local 5G network
(192.168.1.1) to the MAC address (FF:FF:FF:00:00:01) and the IP address
for the intranet (192.168.2.1). Then the IATT translates the destination
IP address for the local 5G network (192.168.7.1) to the IP address for the
intranet (192.168.1.1).

Thus, the two networks with the same IP address range can communicate
each other.

3.2 Tunneling in intranet
To fill the gap in security policy, we propose to use a tunneling technology
in the intranet.

In the proposed method, the tunneling function establishes a tunnel from
the interconnection point to the target server in the intranet. All the traffic
from the local 5G network which goes to the target server is sent through
the tunnel. This limits the area of threat to only the target server which is
protected by anti-virus software. For example, assuming the source terminal
in the local 5G network is infected with malwares, it can only attack the
target server but not the other servers in the intranet.

4 Evaluation
We evaluated the proposed method by prototype software. We utilized an
actual local 5G network and an actual intranet in Hitachi.

4.1 Evaluation setup
We used a local 5G network installed in our open collaborative creation site,
Kokubunji, Japan, which uses a 28 GHz radio channel. The intranet is also
available in this location. On the other side of intranet, we installed a server in a Hitachi’s division in Yokohama, Japan. The server receives images from the client and performs image recognition.

A client system consists of a personal computer (PC), a camera attached to the PC, and a 5G router. The IP address of the 5G router is 192.168.244.4. The intranet IP address of the PC which runs the prototype is 10.1**.1**.11 (masked). The IP address of the server is 10.1**.1**.13.

For the MATT, a pair of the local 5G IP address (192.168.244.4) and the MAC address of the PC is registered, while the IP address for the intranet (10.1**.1**.13) is obtained with DHCP. For the IATT, a pair of the local 5G server address (10.05.90) and the intranet IP address of the PC for prototype (10.1**.1**.11), as the tunneling endpoint, is registered.

For the tunneling we used Secure Shell (SSH) port forwarding for the ease of realization in the intranet. The SSH tunnel is established from the prototype to the server in the intranet (10.1**.1**.13) prior to the evaluation.

We evaluated the following criteria.

1. Whether the inter-layer address translation works, and
2. Whether the tunneled packets are sent only to the target server.

For the evaluation, the incoming and outgoing packets are captured and compared.

4.2 Results
Fig. 3 shows the evaluation results. The window at the left-hand side shows the incoming packets, while the window at the right-hand side shows the outgoing packets.

Fig. 3. Evaluation results; packet capture at local 5G-side NIC (left-hand side) and packet capture at intranet-side NIC (right-hand side).
The packet capture shows that the source IP address for local 5G (192.168.244.4) is translated to the MAC address and IP address for the intranet (10.2**.2**.13) by the MATT. Also, the destination IP address for local 5G (10.0.5.90) is translated to the IP address for the intranet (10.2**.2**.11) by the IATT. The packet capture also shows that the address-translated packets are then tunneled and forwarded to the server (10.1**.1**.13) by SSH port forwarding. Packets to other servers were not observed.

According to the evaluation, we confirmed that the proposed method works properly for the two criteria.

5 Conclusion

In this paper, we proposed an interconnection method between local 5G networks and existing networks, e.g., intranets, by filling two operational gaps between the two networks. The gaps are (1) addressing policy and network management layer, and (2) security policy. We proposed a method consists of two functionalities (1) inter-layer address translation and (2) tunneling in intranet, corresponding to each gap. We implemented this method and evaluated it using an actual local 5G network and an actual corporate intranet. The evaluation result revealed that the proposed method works properly, and the two networks are interconnected.