A Unified Control Architecture for Core–Transport Integration in 6G Networks

Kyungsoo Kim and Namseok Ko
Mobile Core Network Research Section
Electronics and Telecommunications Research Institute(ETRI)
Daejeon, Republic of Korea
{ksjjang, nsko}@etri.re.kr

***Abstract*— In 6G networks, interaction between the core and transport domains is expected to become more flexible and tightly integrated, making real-time, policy-driven path control essential. This paper proposes a novel control architecture centered on the Unified Transport Network Controller (UTNC), a logical control entity that coordinates end-to-end path computation and SID distribution across both core and SRv6-based transport networks. To enable secure and interoperable exchange of transport topology, the architecture extends the existing 3GPP TrafficInfluence API to deliver SRv6 information to the UTNC via the Network Exposure Function (NEF). This design overcomes GTP-related limitations, supports secure interworking in untrusted domains, and provides a scalable and practical foundation for future 6G deployments.**

Keywords—6G, NEF, SRv6, Core-Transport Integration

I. Introduction

Next-generation 6G networks are expected to go beyond ultra-low latency, high reliability, and massive connectivity, placing intelligent services and flexible control architectures at the core of their design. However, current 5G systems maintain a rigid separation between the core and transport networks and primarily rely on the GPRS Tunneling Protocol (GTP) for data forwarding. GTP lacks native support for source routing, policy enforcement, and real-time path visibility, which makes it difficult to meet the demands of dynamic service adaptation, QoS guarantees, and end-to-end network slicing in 6G environments [1]. As a promising alternative, Segment Routing over IPv6 (SRv6) enables source-based routing by encoding path information directly in the packet header, supporting fine-grained traffic control, service chaining, and slice-aware routing [2].

This paper proposes an integrated control architecture for service-based coordination between the mobile core and SRv6-based transport networks in 6G. To support secure interworking in untrusted or multi-domain environments, an extended API interface is introduced via the Network Exposure Function (NEF), allowing the Unified Transport Network Controller (UTNC) to obtain SRv6 topology information and perform policy-based path computation and Segment Identifier (SID) distribution [3].

The proposed architecture addresses key limitations of the GTP-based approach and provides a scalable control model for real-time, intent-aware service delivery in 6G networks.

II. Proposed Architecture Overview

The integrated control architecture proposed in this paper for 6G networks is centered around the UTNC, which is deployed within the control plane of the mobile core network. The UTNC is a novel logical control entity that orchestrates end-to-end path control and SID distribution across both core and SRv6-based transport domains. It integrates topology and policy information to perform real-time, service-aware path computation and resource optimization. Depending on deployment needs, the UTNC may be co-located with the Session Management Function (SMF) or implemented as an independent control function.

The architecture supports both trusted and untrusted transport environments. In trusted domains, the UTNC directly interfaces with the Transport Network Controller (TNC) to retrieve SRv6 topology information. In untrusted domains, the NEF serves as a secure intermediary by extending the 3GPP TrafficInfluence API to receive, filter, and forward validated topology data to the UTNC.

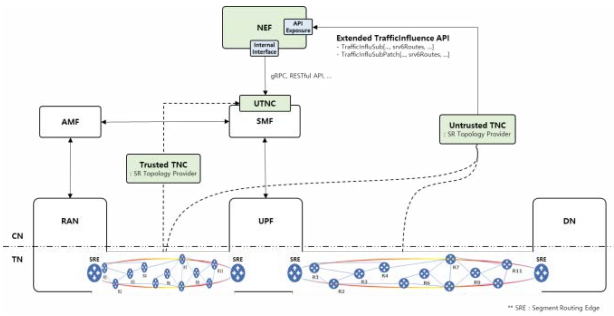

Fig. 1. Control Architecture Supporting Trusted and Untrusted Transport Domains

Figure 1 illustrates the proposed control architecture, which supports both trusted and untrusted transport domains. The UTNC, located in the control plane of the 6G core network, may operate independently or be co-located with existing functions such as the SMF. In trusted domains, the UTNC directly interfaces with the TNC to retrieve SRv6 topology information. In untrusted domains, where the transport network is operated by a third party, the NEF acts as a secure intermediary by extending the 3GPP TrafficInfluence API. The NEF authenticates and filters the topology data received from the TNC before forwarding it to the UTNC.

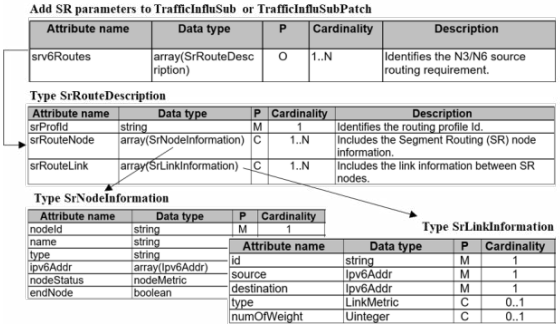

Fig. 2. SrRouteDescription Data Model for SRv6 Exposure

To structure the delivery of this topology data, the architecture defines a new schema, the SrRouteDescription data model, as shown in Figure 2. This model consists of two

primary components: SRNode, which captures the attributes of network elements (e.g., routers, UPFs, gNBs), and SRLink, which defines the logical connections between them. Optional fields such as failure reports and timestamps support fault management and topology freshness. The data is serialized in JSON or Protocol Buffers and delivered to the UTNC via the NEF using extended API mechanisms, ensuring compatibility with existing NEF interfaces while supporting future extensibility.

Based on the collected topology, the UTNC constructs an integrated SRv6-aware network view, performs policy-based path computation, and generates SID lists for core network components including the SMF, UPF, AMF, and RAN. These SID lists are first delivered to the SMF and then propagated to other network entities through standard 3GPP interfaces as follows:

- N4 Interface (SMF → UPF): The SMF delivers the SID list to the UPF using the Packet Forwarding Control Protocol (PFCP). The SID information is included in the Forwarding Action Rule (FAR) and transmitted via PFCP session establishment or modification messages. Based on this, the UPF performs SRv6-based source routing for downlink traffic [4].
- N11 Interface (SMF → AMF): The SID information for uplink traffic is sent from the SMF to the AMF. During initial session establishment, it is delivered via the response to the Create SM Context message; during session maintenance, it is delivered via the SM Context Status Notify message. This allows the AMF to obtain the necessary information for path setup toward the RAN [5].
- N2 Interface (AMF → RAN): The AMF includes the received SID list in the NGAP PDU Session Resource Setup or Modify Request message and forwards it to the RAN (gNB). The RAN then uses the SID list to perform SRv6-based source routing for uplink traffic from the UE [6].

III. Path Computation and Control Procedure

The UTNC constructs a unified network topology that integrates the mobile core and transport networks, based on SRv6 topology information received from the NEF or TNC. Using this topology, the UTNC computes optimal paths according to service requirements such as bandwidth, latency, and reliability, and generates them in the form of SRv6 SID lists. In addition to traditional algorithms such as Dijkstra, AI-based prediction models can also be applied depending on traffic characteristics and QoS constraints, enabling more flexible and adaptive path control.

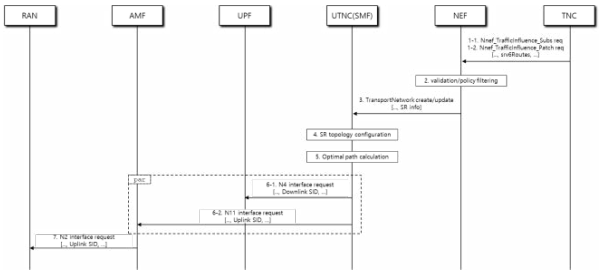

Fig. 3. SRv6 Interworking Procedure in Untrusted TNC

Figure 3 illustrates the UTNC-based path computation and distribution procedure in the form of a sequence diagram. It shows the step-by-step flow from SR information acquisition to path calculation and SID distribution across user-plane components. The SR topology information delivered from the TNC via the NEF is used as input for integrated topology construction and path computation by the UTNC. The resulting SID list is then applied to the user plane through standard 3GPP control interfaces such as N4, N11, and N2. This procedure demonstrates that the proposed architecture can maintain compatibility with the existing 5G system while enabling flexible, policy-based path control.

IV. Conclusions and Future Work

This paper has presented a NEF-integrated control architecture for 6G networks that enables flexible coordination between the mobile core and SRv6-based transport domains. At its core is the UTNC, a policy-driven control entity that orchestrates path computation and SID distribution while leveraging the programmability of SRv6 to address key limitations of GTP-based models. Through an extended TrafficInfluence API, the NEF securely exposes SRv6 transport topology even in untrusted domains, while maintaining compatibility with standard 3GPP interfaces such as N4, N11, and N2. The architecture enables lightweight path control and scalable integration, and its modular design supports flexible deployment and future evolution toward federated or hierarchical UTNC structures.

Despite these advantages, the asynchronous nature of NEF-based communication may pose latency and responsiveness challenges for real-time services. Future work will focus on optimized interworking mechanisms and on validating the proposed architecture through prototype implementation and quantitative performance evaluations (e.g., latency, throughput, scalability).

As 6G networks evolve toward greater autonomy, intelligence, and flexibility, the proposed control architecture offers a practical and standards-aligned foundation for enabling real-time, policy-driven path control at scale. The integration of transport programmability and secure API-based exposure mechanisms represents a significant step toward realizing intent-aware, end-to-end optimized 6G service delivery.

Acknowledgment

This work was supported by the ICT R&D program of MSICT/IITP. [RS-2024-00405354, Development of Evolved SBA Framework and Core Technologies of Control/User Plane NFs]

References

[1] S. Matsushima et al., “A Transport Network-Aware Mobility Management System for Segment Routing-Based Mobile Networks”, RFC 9433, IETF, 2023.

[2] C. Filsfils et al., “Segment Routing: Applying Source Routing to Modern Networks”, IEEE Communications Magazine, 2017.

[3] 3GPP TS 29.522, Service Communication Function and NEF; Stage 3, Release 18, V18.2.0, June 2024.

[4] 3GPP TS 29.244, Interface between the Control Plane and the User Plane Nodes; PFCP Specification, V18.4.0, June 2024.

[5] 3GPP TS 29.502, 5G System; Session Management Services; Stage 3, V18.4.0, June 2024.

[6] 3GPP TS 38.413, NG-RAN; NG Application Protocol (NGAP), V18.4.0, June 2024.