Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 21 January 2026

Chenchen Yang,
Huanhuan Huang,
Arashmid Akhavain,
Faye Liu,
Xueli An,
Weijun Xing,
Huawei
Jinyan Li,
Aijun Wang,
China Telecom
Wencong Yang,
China Unicom
20 July 2025

Requirements and Enabling Technologies of Agent Protocols for 6G Networks
draft-hw-ai-agent-6g-00

Abstract

Agent application will be surely the common trend for a long time in future, while agent protocols are so popular that more and more protocols are being worked out. The telecommunication industry plays a pivotal role in the Agent ecosystem. The overall technology success hinges on how telecommunication industry could adopt the latest AI trends in order to handle its specific usage scenarios and performance requirements, e.g., in the coming 6G era. This document will provide the first attempt to analyze the agent protocol requirements and relevant enabling technologies based on mobile communication system specific characteristics.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 21 January 2026.

Table of Contents

1. Introduction

6G as the next generation mobile communication technology will play an essential role in the entire society digitalization process. On one hand, 6G will provide better connectivity compared to 5G, and on the other hand, 6G will go beyond connectivity, for instance, features like native-AI and integrated communication and sensing will enable new business revenues. It could be expected that enormous amount of new use cases and services could be enabled by 6G. However, increased new features as well as increased demands of various use case scenarios will also bring challenges on 6G system design. For instance, how to enrich Telco scope services but remain operationally efficient? How to provide per user network customization without scaling up the service provisioning complexity? How to speed up new service delivery and identify relevant standardization requirement to ensure interoperability?

Carrying these questions in mind, 6G is seeking answers by utilizing promising technologies like agentic AI (empowered by foundation model), which gained a lot of attention in recent years. Agentic AI technology is rapidly evolving as businesses embrace autonomous systems to streamline operations, enhance decision-making, and personalize/customized user experiences. Therefore, agentic AI could become the essential cornerstone of 6G [1]. Such technology trend is quickly adopted by telecommunication field, for instance, ETSI and 3GPP have launched relevant studies in this scope. ETSI outlined its vision of AI Agent based Core network in [2] and provided a detailed study on use cases and requirements in [3]. 3GPP studied agent services in 3GPP R20 SA1 [4]. Moreover, the work task#3 on AI and agent has been adopted in 3GPP SA2 6G SID [5].

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Characteristics of Mobile Network

2.1. Resource dynamicity

Mobile networks provide wireless connectivity services in a dynamic environment with resource volatility and link unreliability. To deliver high-quality connectivity services, networks utilize adaptive mechanisms such as real-time resource scheduling, multipath transmission, and dynamic retransmission schemes to mitigate the uncertainty of radio resources and links. Unlike fixed networks with static infrastructure, mobile systems must continuously calibrate resource allocation to maintain link quality and ensure resilience while sustaining service continuity for diverse applications.

2.2. Guaranteed Quality of Service (QoS)

Guaranteed QoS is a fundamental design principle in mobile networks, enabling customized performance to meet heterogeneous application demands. By establishing differentiated resource priorities, networks enforce strict guarantees:ultra-reliable low-latency transmission for critical industrial data transmission, prioritized bandwidth allocation for real-time services (e.g., voice calls, video conferencing), and flexible throughput for non-urgent traffic (e.g., email, file downloads). Such differentiation is also extending to multi-modal services, e.g., XR service and digital twins, enabling consistent performance across use cases and empowering mobile networks as unified platforms for diverse digital services.

2.3. Mobility

Mobility management, a core feature of mobile networks, enables continuous connectivity as terminals move across different locations. Networks trigger seamless handover based on the radio conditions to maintain communication without interruptions. Sometimes network could allocate resources in advance by prediction to reduce latency during transitions. This comprehensive mobility management framework supports various usage scenarios, from stationary to high-speed mobility and cross-regional roaming, making mobile networks essential for critical applications that require constant access.

2.4. Multi-domain Interoperation

Mobile communication network is multi-technology and multi-business domain in nature and it is important to establish a cohesive connectivity ecosystem for different network operators, network tenants and service providers. From the technology perspective, inter-operator roaming leverages standardized protocols to empower subscribers to access partner networks, ensuring seamless global connectivity. Even within the same Mobile Network Operator (MNO) environment, different network tenants can share the network under the control of the MNO to achieve a better service performance especially for 6G new services like sensing, AI and computing. On the other hand, cross-domain collaboration supports mobile communication network and Over-The-Top (OTT) service providers to exchange capabilities via capability exposure to provide better services for end users. This interoperability not only enhances resource utilization but also unlocks novel use cases, facilitating the development of a unified, scalable network infrastructure that supports diverse applications.

2.5. Security, Privacy and Trust

The security capabilities of each generation are continuously improving. The security architecture defines security domains, end-to-end security mechanism, roaming security, and backward compatible security measure. Achieving a balance between security and service performance is the principle for security capability design. Supporting multiple security mechanisms and being able to switch between them is essential.

Privacy preservation can be achieved by encryption, anonymization, zero-knowledge proofs, privacy computing, etc. The network provides users with privacy protection based on the data lifecycle.

In terms of trust, the centralized trust model and the 3rd party endorsement model co-exist alongside with the multi-lateral trust model. The first two trust models provide single-point trust. The latter multi-lateral trust model offers multiple roots of trust/ consensus trust, which facilities the fast establishment of cross-trust domain connections.

2.6. Session-level Operation

In conventional mobile communication network design, PDU session serves as the fundamental granularity for connectivity service management. Through session management, mobile networks perform resource allocation and policy enforcement at the QoS Flow level, where individual service flows (e.g., video calls, IoT telemetry, or cloud gaming streams) are mapped to dedicated QoS flows with specific performance characteristics. Session management systems continuously monitor Key Performance Indicators (KPIs) such as data rate, latency, and packet loss ratio, enabling dynamic resource adjustment to maintain connectivity service performance. This session-level operation effectively bridges end-user QoS requirements with network resource optimization, making it a key part of network design.

2.7. Systems Coexistence

In the actual deployed commercial networks, systems based on legacy and state of the art standards operate concurrently due to gradual deployment cycles, varying terminal lifespans, and global differences in upgrade timelines. For example, in some regions, 4G and 5G networks are operated alongside even older 3G systems. Even within a single generation, almost every 1 or 2 years, a new release is published and some features are updated accordingly. The coexistence of systems from different generations and releases presents challenges especially considering the backward and forward compatibility.

3. Agent Protocols Requirements

3.1. Multi-agent system covering terminal, network and service

As proposed by ETSI [2], agentic AI technology could innovate the mobile communication network architecture design, and 6G core network could be established as a multi-agent system. There will be a broad scope of agents, for instance 3GPP specified agents versus non-3GPP agents, network agents versus UE agents, etc. These agents interact and collaborate with each other to form a new communication paradigm, and they could invoke different types of resources to support the communication. Such resource could be for instance toolbox, memory, connectivity resource, computing resource, etc. Under this context, 6G goes hand in hand with agentic AI technologies. 6G may utilize agent protocols and relevant enabling technologies to enable the following mobile network specific scenarios:

1. *6G network agents interaction:* 6G network internal agents collaborate with each other, and invoke relevant resources;

2. *UE agent/resource and network agent/resource:* 6G network agent and UE agent collaborate with each other, 6G network agent invokes resources on UE side, or vice versa;

3. *Service exposure:* Expose 6G network agent services and resources to 3rd parties;

4. *Service consumption:* Consuming agent services and resources from 3rd parties.

3.2. QoS Assurance for Multi-agent Communication

Agent traffic as the following characteristics:

3.2.1. Agent traffic may consist of multiple “Parts” and multi-modal data：

Multi-agent communication traffic can contain several “Parts” (e.g., the smallest unit of content within a Message or Artifact [6]). The data types of different Parts may be different and multi-modal (e.g., text, file, document, image, structured data, real-time audio stream, video streaming).

The sizes of different Parts can be different and the transmission modes may be also different (e.g., real-time steaming, Server-Sent Events (SSE), or Push Notification).

Given these traffic characteristics above, dedicated QoS framework should be designed for better performance.

3.2.2. Heterogeneous QoS requirements among multiple “Parts”：

Heterogeneity between Messages and Artifacts: An agent service flow may contain Messages and/or Artifacts, their QoS requirements are different, e.g., the Message’s requirement (e.g., timeliness, accuracy, delay) is stricter.

Heterogeneity for “Parts” within a same Message or Artifact: The QoS requirement (e.g., delay, deadline to be sent to peer endpoint) for the different Parts of a same Message or Artifact may be the same or not.

3.2.3. Burst Agent traffic

Agent service flow can be burst traffic: dynamic QoS should be guaranteed and network resources should be adjusted in real-time when the agent service flow is burst traffic instead of periodic traffic.

The characteristics of agent traffic above provides possibilities to optimize QoS schemes and resource scheduling. The overall QoS of an agent service flow should be guaranteed while the network resource consumption is minimized. Parts with different QoS requirements may be sent via different resources. For example, network resource allocated to Parts of SSE/Streaming mode should keep active all the time, but network resource allocated to Parts of Push Notification mode can be (de)activated (e.g., released or suspended) flexibly. The 6G network can adjust the resource scheduling and management mechanism based on the different modes.

3.3. Agent Service Continuity

The continuity of agent service (e.g., message or task processing result) should be guaranteed, e.g., in the mobility scenario for UE-agent, or when the network addressing are changed. Additional singling overhead for link (re)establishment and connectivity disruption possibilities should be reduced. For instance, how to wake up the equipment that hosts the agent. Agent instances can be deleted or moved from one device to the other. Mobility handling in such situations need to be carefully tackled. In addition, assume that we have an agent on equipment that is currently running a task. In the middle of the task, the equipment shuts down, but before it does, the agent should be moved (sent) to another hosting equipment. How to handle this situation and how the agent is notified?

3.4. Agent Task-Oriented Resource Management

The interaction between agents is typically task-oriented, where task is a collection of actions to satisfy the user requirements. An agent (i.e. agent client) may request another agent (i.e. agent server) to perform a task [6]. It can query the task status during the execution process and receive the results upon task completion.

As described in section 2.6, the mobile network operates based on sessions. The traditional mobile network mainly performs communication resource management to establish the UE-oriented sessions and guarantee the QoS of a connectivity for a UE. However, in an agentic system where multiple agents may collaborate to perform a task, the network shall manage and schedule multi-dimensional resources (such as communication resource, AI resource, computing resource, data resource, etc.) to guarantee the QoS of a task.

Thus, a task session is required to support the communication of different agents in network. And the network schedules resource and guarantees QoS based on task granularity. Task information, e.g., task identifier, needs to be carried when Agents exchanges message or task results, to associate with the corresponding task.

3.5. Intent-based Interaction

AI Agent is an automated intelligent entity capable of reasoning, decision-making, executing tasks autonomously to achieve a specific goal. A consumer provides the high-level goal description that needs to be realized, instead of the step-by-step execution instruction, based on which the agent can make execution plans through the local AI model and invoke the proper tools to perform the task. Thus, Agent protocols should support Agents to interact with each other or with consumers through intents, to make the agent interaction flexible enough.

3.6. Security, Privacy and Trust

The security control flow provides the access security control, the secure transportation, and the cross-domain secure collaboration capabilities, which is also important to agent protocol, as agents will be one of the main communication end-point for both terminal and network. Various cryptographic algorithms ensure the security of transmission channels and the implementation of different levels of security measures according to different policies.

The transmission of user consent and service visibility messages between the network and the terminal side ensures that the subscribers can be aware of the data usage purposes agreed upon between the operator and the subscriber. AI Agent brings new possibility to interact with each other with multi-modal information, in this case, the procedure of user consent and service visibility would not be ignored.

3.7. Agent Governance

AI Agents of different skills, capabilities, and vendors need to discover each other when they collaborate to perform a task. It is important to manage and control the agent information to enable an agent to find others from a massive number of candidates.

The agent protocol has to support the agent (de-)registration, update and discovery with an authority that may be deployed in central or distributed way. It needs to consider how this authority to ensure agent behaviors, agent skill set or capability publish, ensure trustworthiness and discovery among agents, when designing the protocols.

The effective publish-subscribe and request-response mechanisms for discovering agents with required skills or capabilities are needed. Wake up calls of equipment that hosts the agents need to be supported as well. This is also related to service continuity which should be maintained by the agentic ecosystem.

3.8. Backward Compatibility and Forward Compatible

As mentioned in 2.4 and 2.7, networks consist of multiple stakeholders/parties with various UE, network, and protocol versions. Therefore, agent protocols should be flexible, backward-compatible, forward-compatible, potentially self-evolving (e.g., protocol self-generation and negotiation, protocol version self-upgrade or merge) in the future, and easy to evolve. More specifically, agent protocols should be built upon existing network functions and systems, while also remaining adaptable to future network architecture/functions designs and system evolutions.

3.9. Extensibility

Agent protocols exist across multiple domains, such as UE, RAN, CN, and DN. Additionally, service, data, and capability exposure may originate from different networks. Therefore, agent protocol should support the expanding and scaling of agents so that any type of agents (e.g., Network autonomy agent and integrated sensing-AI Agent) can be seamlessly integrated to the whole agent system. To achieve this, task-based communication should be supported to enable rapid service subscription and publishing between agents. ## Flexibility AI Agents are capable of self-learning and self-evolving, which implies that skills, capabilities, and accepted input and output modalities may change as time goes. The agent protocol shall be designed to be sufficiently flexible, allowing fast adaption to expected changes.

Moreover, the protocol data objects and agent profiles exchanged within the protocol shall be designed with flexible fields that are easy to scale and modify without re-design.

3.10. Isolation

The messages or traffic flows of mobile network usually have different-level of security or delay requirements. For example, request messages from UE have higher security requirement than that for common traffic flows. Thus, agent messages or traffic flows with different performance requirements shall be decoupled and isolated to facilitate differentiated processing.

3.11. Tool Invocation

The key feature of an agent is that it can invoke tools to execute tasks autonomously. When AI Agents are introduced into 6G network, various network capabilities, network functions and even the 3rd party application functions can serve as tools to be invoked and used by agents.

It is an important aspect to enable agents to invoke the required tools accurately. Thus, it needs to consider how to enable the Agent protocols to describe tools' information explicitly and sufficiently such that agents can easily identify target tools and easily learn how to use them.

Different tools have different implementation methods and invocation approaches. How to enable agents to flexibly invoke different tools to support plug-and-play of future tools also needs to be considered.

3.12. Knowledge Retrieval

AI Agents need flexibly access to 6G network internal or external data sources or knowledge bases to retrieve additional information that may not be present within the local knowledge of an agent model. The following issues need to be considered for Agent protocol design:

* *Metadata filtering:* how to filter the un-related data, e.g. through time label, data type label.

* *Data representation:* how to represent data of knowledge so as to improve transmission efficiency, such as represented as vectors or graphs.

* *Retrieval mechanism:* how to search and retrieve the required data, e.g. through similarity, key words, Token, natural language, etc.

4. Enabling Protocol Technologies

Given the agent protocol requirements elaborated above, the following enabling technologies can be investigated and standardized in IETF, e.g., in terms of Agent governance layer, Meta protocol layer, Security control layer, and Transport layer. Different features should be provided in each layer, which will also be investigated and introduced by 3GPP potentially.

4.1. Agent Governance Layer

4.1.1. Registration and Discovery

As shown in section 3.7, an authority is required to govern the available AI Agents in the mobile network. The new agent will register its agent profile to the authority, request to update the agent profile when the agent skills or capabilities are changed, and de-register from the authority when the agent is not used anymore. The agent profile contains the key information about the agent, such as agent role description, skills, capabilities, identifier, input and output schema, vendor information, URL, etc.

The authority will store and maintain the agent profile of all the available agents. When an agent wants to discover a target agent by providing required agent description, the authority needs to perform a search and matching between the provided description and the role or skill description of registered agents, e.g. through cosine similarity computation or Jaccard similarity computation [7][8].

4.1.2. Publish and Subscribe

The AI Agents can subscribe to the authority about the agent information of specific set of agents so as to acquire their real-time updates. The agent subscription can support various forms, such as through agent ID, role type, skill type, etc.

When the profile of an agent is updated or the agent is de-registered, the authority shall notify the other agents that subscribed to the information of this agent as to prevent them from sending inappropriate requests to the agent.

In addition, if there is no registered agent can perform the task requested by an agent, or all available agents are in regions where the request agent cannot render the task, the agent ecosystem can also provide a registration mechanism such that an agent posts its interest and gets notified as soon a new suitable agent comes and registers with the ecosystem and comes online.

4.1.3. Agent Communication

In the mobile network, an agent may need to communicate with other agents, resources (e.g., tools, data, or APIs), underlying infrastructure (e.g. base stations, computing platform), and users (e.g. UEs, applications). For different communication objects, various protocol methods and data objects are needed to be defined. To enable the flexible and intent-based interaction for agents, the data objects are usually semi-structured, where the contents or

values of each field are not pre-defined and only the key labels are inserted to improve the understandability and completeness.

For the communication between agents, Google A2A defines several methods based on JSON RPC 2.0, such as _message/send_, _task/get_, _task/cancel_ [6], to support initiating a new task, updating or deleting an existing task, querying the current status of a task, subscribing the information of specific tasks. The data object "_Task_" is exchanged with the methods, which includes the information such as task identity, requirements, context, states, outputs, etc. They can be applied to the mobile network with proper extension combining mobile network characteristics. For example, the task QoS information, network status and resource information also need to be exchanged. And an agent can also refuse a task due to reasons such as limited network resources and transmission buffer.

For the communication between agents and resources (such as tools, data, APIs), the methods need to support AI Agents to invoke various network and service functions, in order to trigger and execute suitable network actions and operations, or to query network operator data, network running log data, beyond connectivity data (e.g., sensing data, AI data), etc.

The methods for the communication between agents and users are required to support a user to request a service (e.g. AI, sensing), update or release a service, acquire the service status or result, etc.

4.1.4. Multimodal Data Management

The data exchanged by agents are multi-modal, which can be text, image, audio, video, structured data, etc. For example, A2A protocol defines three types of data structures [6], i.e., TextPart, ProfilePart and DataPart, to respectively carry texts, profile and structured data. More kinds of data structures, such as AudioPart and VideoPart, may be needed, e.g., a UE may initiate a request to the agent in the mobile network through audio. Agent protocols should be designed with the principle that the Agent data with different modalities can be distinguished, based on which 6G network can provide differentiated QoS assurances. For example, on one hand, the Agent protocol can support to encapsulate data of different modalities to distinct data structures. On the other hand, the 6G network may establish different resources for transmitting various modalities of data to perform QoS control and guarantee.

Besides, there shall be a closely integration design between the agent ecosystem and the underlying network. For example, the equipment hosting the agent may enter sleep mode when the agent is

not executing task, and it needs to be woken up by a client agent so that the server agent can process the multi-modal data from the client agent to perform the task.

Multi-modal data is heterogeneous, meaning that data from different modalities differ in structure, semantics and representation, but they complement each other from various perspectives on the same subject. Processing and analysis of multi-modal data are quite challenging, which requires to consider multiple impact factors, such as data alignment, feature extraction, etc. Thus, the following key technologies shall be adopted.

- Data pre-processing technology: it includes data cleaning (removing noise and redundant data), data standardization (converting data from different modalities into a unified format), data augmentation (increasing the diversity of data through operations such as rotation, scaling).

- Feature extraction technology: it includes text, image, audio, video feature extraction, etc.

- Data alignment technology: it is to ensure the consistency of data across time, spatial location, and semantics.

- Fusion technology: it is to integrate diverse data to enhance its completeness, accuracy, and usability.

* *Data pre-processing technology*: it includes data cleaning (removing noise and redundant data), data standardization (converting data from different modalities into a unified format), data augmentation (increasing the diversity of data through operations such as rotation, scaling).

* *Feature extraction technology*: it includes text, image, audio, video feature extraction, etc.

* *Data alignment technology*: it is to ensure the consistency of data across time, spatial location, and semantics.

* *Fusion technology*: it is to integrate diverse data to enhance its completeness, accuracy, and usability

4.2. Meta Protocol Layer

As mentioned in 3.8, 3.9 and 3.10, agent protocols should allow for customization or privatization of the protocol while maintaining the standardized agent protocols. Capabilities such as self-negotiation, self-generation and self-evolving of agent protocol should be supported to solve the compatibility problem, while protocol release control is required to accommodate the co-existence of multi-releases of those cross-operator and cross-domain agents. Additionally, agent protocols should be able to call tools and data by calling network functions.

Meta protocol layer should support the self-negotiation of agent [9]. Agent itself can decide the modality of interaction message like text, voice, etc.

Considering the co-existence of multi-party and cross-domain agents inside of the whole agent system, both the standardized protocol and negotiated protocol can be potential options.

4.3. Security, Privacy and Trust Layer

As mentioned in 3.6, agent protocols should consider the requirements of security, privacy and trust. Some of the enabling technologies are listed as below:

- Distributed Identity (DID) system for AI Agents

Based on the mobile network oriented DID system, the network offers rapid authentication and key establishment based on multiple roots of trust, fine-grained authorization, and selective privacy disclosure via agent protocols. Simultaneously, the DID system supports the security of cross-domain, e.g. working for different groups of AI Agents, connections through the same DID translation and related policies.

- Distributed ledger

Distributed ledger technology provides a foundation of trust for multi-party collaboration, which will be common case for AI Agents ineraction. Acting as a bridge of trust, it enables different systems holding credentials issued by various authoritative institutions to achieve mutual trust. As a consensus infrastructure, it offers tamper-proof functionality and transparent auditability for critical information.

- Ciphertext-based computing technology

Considering the elimination of user privacy concerns, ciphertext-based computing technology provides the capability of "computing without knowing" for network queries and computations on user data. Agent protocols should include this option to ensure that data privacy at different levels can be handled in an acceptable manner.

- Quantum-safe technologies

Quantum-safe technologies include post-quantum cryptography (PQC) and its protocols based on cryptographic techniques, as well as quantum secure transmission methods such as Quantum Key Distribution (QKD). The preemptive deployment of quantum-safe technologies, such as PQC migration, will prepare for defending against quantum attacks. The algorithm set for agent protocols should consider quantum-safe from day 1.

4.4. Transport Layer

As mentioned in 3.2, 3.3, 3.4 and 3.11, the Agent QoS and service continuity should be guaranteed. Agent messages or traffic flows with different performance requirements shall be decoupled and isolated. The following potential technologies for transport layer protocols can be investigated:

* *To support stream multiplexing, collaboration and grouping:* e.g., different “Parts” of agent traffic with different sizes can be sent in parallel via a group of transport streams to enable them to arrive to peer node synchronously within a strict delay budget, or sent asynchronously with different priorities within a same stream if synchronous arrival to peer node is not needed. The balance between the complexity of transport connection establishment and the flexibility of scheduling should be considered.

* *To support a reliable and efficient transmission mechanism for agent traffic:* A) Stream multiplexing of multiple agent traffic data streams, B) Traffic steering, switching, splitting of multiple agent traffic data streams.

* *To natively support connection migration, quick link establishment*: so that agent service continuity could be guaranteed in mobility scenarios.

* *To support burst agent traffic transmission*: Burst traffic information can be encapsulated in protocol header for better QoS guarantee and resource real-time scheduling and adjustment. The QoS (e.g., latency and timeliness) is guaranteed toward the whole burst data set of agent traffic rather than a specific packet.

5. Summary

A hierarchical consideration of agent protocol is definitely important to meet different kinds of requirements, e.g., from 6G network. Collaborations between IETF, ETSI and 3GPP and collaborations across different work groups (e.g., for agent protocol, transport protocol, and security) of IETF are required.

6. Reference

6.1. Informative References

[1] Li, Xu, Weisen Shi, Hang Zhang, Chenghui Peng, Shaoyun Wu, and Wen Tong. "The Agentic-AI Core: An AI-Empowered, Mission-Oriented Core Network for Next-Generation Mobile Telecommunications." _Engineering_ (2025).

[2] ETSI GR ENI 051 V4.1.1, “Experiential Networked Intelligence (ENI); Study on AI Agents based Next-generation Network Slicing”, 2025.02.

[3] ETSI ENI ISG 055 Early Draft, “Use Cases and Requirements for AI Agents based Core Network”, 2025.06.04.

[4] 3GPP TR 22.870 (V0.2.0): “Study on 6G Use Cases and Service Requirements; Stage 1 (Release 20)”.

[5] 3GPP SP-250806: "Study on Architecture for 6G System".

[6] A2A Protocol. "Specification". https://a2a-protocol.org/latest/specification/, 2025.

[7] D. Gunawan, C. A. Sembiring, M. A. Budiman, “The implementation of cosine similarity to calculate text relevance between two documents”, Journal of physics: conference series, 2018.

[8] S. Bag, S. K. Kumar, M. K. Tiwari, “An efficient recommendation generation using relevant Jaccard similarity”, Information Sciences, 2019.

[9] Marro, Samuele, Emanuele La Malfa, Jesse Wright, Guohao Li, Nigel Shadbolt, Michael Wooldridge, and Philip Torr. "A scalable communication protocol for networks of large language models." arXiv preprint arXiv:2410.11905 (2024).

7. Security Considerations

This document should not affect the security of the Internet.

8. IANA Considerations

This memo includes no request to IANA.

9. Appendix

10. Normative References

[RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <https://www.rfc-editor.org/rfc/rfc8986>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

Authors' Addresses

Chenchen Yang,
Huawei
Lianqiu Lake, Qingpu District
Shanghai
201799
China
Email: yangchenchen7@huawei.com

Huanhuan Huang,
Huawei
Lianqiu Lake, Qingpu District
Shanghai
201799
China
Email: huanghuanhuan9@huawei.com

Arashmid Akhavain,
Huawei
303 Terry Fox Drive, Kanata
Ottawa K2K 3J1
Canada
Email: arashmid.akhavain@huawei.com

Faye Liu,
Huawei
9 North Buona Vista Dr.
SINGAPORE 117674
Singapore
Email: liufei19@huawei.com

Xueli An,
Huawei
Riesstr. 25
80992 Munich
Germany
Email: Xueli.An@huawei.com

Weijun Xing,
Huawei
Lianqiu Lake, Qingpu District
Shanghai
201799
China
Email: xingweijun1@huawei.com

Jinyan Li,
China Telecom
Beiqijia Town, Changping District
Beijing
102209
China
Email: lijinyan@chinatelecom.cn

Aijun Wang,
China Telecom
Beiqijia Town, Changping District
Beijing
102209
China

Email: wangaj3@chinatelecom.cn

Yang Wencong,
China Unicom
No. 9 Shouti South Road, Haidian District
Beijing
100044
China
Email: yangwc27@chinaunicom.cn