GTI Agent Protocols for Mobile Communication Networks White Paper

GTI Network Agent Protocols for Mobile Communication Networks White Paper

Version:	v1.0
Deliverable Type	□ **Procedural Document** ☐ **Working Document**
Confidential Level	☑ **Open to GTI Operator Members** ☑ **Open to GTI Partners** ☑ **Open to Public**
Program	**Network and AI**
Working Group	**N/A**
Project	**Project 1: Network Intelligence**
Task	N/A
Source members	China Mobile, Turk Telekom, ANP Open Source Community, CATT, China Southern Power Grid, Cygnusemi, DEEP Robotics, Digit Technology, Hongdian, Huawei, Humanoid Robotics Association Switzerland, Midea Group Co., Ltd. , Nokia, OPPO, Oray, Rokid, Shanghai MScape Technology Co., Ltd., State Grid Shandong Electric Power Company, Information & Communication Company, TD Tech, UBTECH ROBOTICS CORP LTD, vivo, ZTE
Support members	China Mobile Research Institute, Turk Telekom, ANP Open Source Community, CATT, China Southern Power Grid, CSG Digital Grid Group Information &

	Communication Technology, Cygnusemi, DEEP Robotics, Digit Technology, Hongdian, Huawei, Midea Group Co., Ltd. , Humanoid Robotics Association Switzerland , Nokia, OPPO, Oray, Rokid, Shanghai MScape Technology Co., Ltd., State Grid Shandong Electric Power Company, State Key Laboratory Of High-end Heavy-load Robots, Information & Communication Company, TD Tech, UBTECH ROBOTICS CORP LTD, vivo, ZTE
Editor	Zhenning Huang
Last Edit Date	2026-06-22
Approval Date	2026-06-22

Document History

Date	Meeting #	Version #	Revision Contents
2026-06-23	#45	1.0	Version 1.0

Foreword

With the rapid advancement of artificial intelligence technology, agents are becoming the core driver for the large-scale deployment of AI, leading to the evolution of mobile network connected entities from "humans and devices" to "humans, devices, and agents". However, the existing agent communication protocol ecosystem is highly fragmented and predominantly designed for internet application scenarios, making it difficult to meet the requirements of mobile communication networks for wide-area mobility, cross-domain collaboration, and security control. There is an urgent need to define a standardized, cross-domain interoperable, secure, and extensible agent communication protocol.

This white paper is the result of experts' exploration and practice in deeply integrating communication networks with agents. It covers the following main areas: First, it analyzes the communication requirements of agents across several scenarios, including smart personal life, high-end industrial manufacturing, public safety, and network-native intelligence, and reviews the industry progress on agent protocols, distilling six core challenges of cross-domain identity mutual recognition, cross-ecosystem capability discovery, multi-principal task collaboration, multi-modal differentiated transmission, protocol adaptation and interoperability, and telecom-grade security management. Second, it proposes the core philosophy of "compatibility and inclusiveness, layered decoupling, dynamic adaptation, and security and trustworthiness" for agent protocols in mobile communication networks, and presents a design organized around six dimensions of foundational transport, identity and identification, capability discovery, task coordination, intent interaction, and security protection. Finally, it looks ahead to the evolution direction of agent communication protocols and the path for industry collaboration, providing references and guidance for technology deployment and standardization.

China Mobile hopes to work closely with equipment vendors, vertical industries, research institutions, and other industry partners, guided by scenario-specific requirements, to jointly refine the core specifications for inter-agent communication, promote standardization and interoperability of protocols, prevent fragmentation of protocol and technology stacks, and together drive the transformation of communication networks from "pipeline connections" to "intelligent service hubs" — achieving a leap from the Internet of Everything to the interconnection of billions of agents.

Table of Contents

1 Introduction

Against the backdrop of accelerating global technological revolution and industrial transformation, agents, which are the core driver for the large-scale deployment of Artificial Intelligence (AI) technology, are becoming a strategic focal point in technological competition and industrial upgrades across the globe. China has incorporated artificial intelligence into the key cultivation directions of "new quality productive forces." The 15th Five-Year Plan proposal explicitly calls for the comprehensive implementation of the "AI+" initiative, leveraging AI to lead the transformation of research paradigms, seize the high ground in industrial applications, and comprehensively empower all industries. Relevant ministries including the Ministry of Industry and Information Technology have also issued a series of policies in rapid succession, clearly supporting R&D in frontier technologies such as agents and embodied intelligence, promoting cross-domain intelligent collaboration and protocol standardization, and providing strong policy support for agent technology innovation and industrial application.

At the same time, global agent technology and applications are experiencing explosive growth. From the rapid iteration of application-layer protocols such as Anthropic's Model Context Protocol (MCP) and Google's Agent2Agent (A2A) protocol, to continuous innovation in terminal forms such as industrial robot clusters, personal digital assistants, and intelligent inspection devices, the role of agents has evolved from single-task execution to cross-scenario, cross-ecosystem group collaboration. A full-spectrum development pattern of "embodied + wearable + virtual" is gradually taking shape, enriching the traditional entities of “human and device” in communication networks with agents, opening a new era of "Interconnection of a Billion-Agents."

The large-scale deployment of agents is leading to a fundamental shift in communication principals, which traditionally involves humans, terminals, and applications, toward embracing agents with autonomous decision-making, task collaboration, and continuous evolution capabilities. Agents are gradually becoming more active communication principals than humans, terminals, or applications. Novel intelligent agent terminals such as AI glasses, embodied intelligent robots, and personal digital assistants are continuously emerging, not only reshaping terminal form factors and business models, but also posing new demands on the connectivity, enablement, and management capabilities of communication networks.

In this landscape, the ecosystem fragmentation of agent communication protocols is becoming increasingly prominent. Since 2023, the industry has released over 20 agent communication protocols, which differ significantly in their design philosophy, technical architecture, and functional implementation. The absence of unified standards and specifications makes it difficult for agents to achieve efficient and secure interconnection, and cross-domain collaboration. Moreover, existing protocols are mostly designed for IT application scenarios and are insufficiently adapted to the needs of mobile communication networks. As new intelligent terminals such as drones and embodied intelligent robots accelerate their integration into networks, existing communication protocols urgently need to be strengthened in terms of bandwidth assurance, low-latency transmission, and security control. To this end, there is a pressing need to define standardized agent communication protocols that support wide-area interconnection, cross-domain interoperability, and secure extensibility to facilitate the large-scale deployment of multi-agent collaboration.

2 Scenarios and Challenges for Agent Communication in Mobile Networks

2.1 Scenario Requirements

2.1.1 The Era Is Calling: Agent Applications Are Emerging in Abundance

Agent application scenarios are evolving from single-task execution to multi-principal collaboration, covering multiple domains including smart personal life, high-end industrial manufacturing, public safety, and network-native intelligence. Different scenarios impose differentiated demands on agent communication in terms of real-time performance, reliability, collaboration, and security.

1) Smart Personal Life: An All-Around Personal Life Assistant

Users issue composite tasks such as "clean the living room" or "start patrol at the campsite" to a personal AI assistant via natural language, which then coordinates multiple home agents to complete task decomposition, execution, and feedback. In this scenario, the user, personal AI assistant, robot vacuum, robot dog, drone, AI glasses, home AI server, and third-party software agents potentially have communication roles.

Key communication requirements:

- Identity and authentication: Assign globally unique digital identities to agents, supporting cross-network routing and mutual identity recognition;
- Capability registration and intent-based capability discovery: Agents register capabilities to the communication network, which matches appropriate agents based on intent;
- Agent task collaboration: Support session context management, master-slave task allocation and state synchronization, and real-time task feedback delivery;
- Cross-platform and cross-ecosystem interoperability: Support interconnection between agents from different platforms and ecosystems;
- Multi-modal transmission adaptation: Support efficient transmission of multi-modal data including 4K video, audio, images, and text.

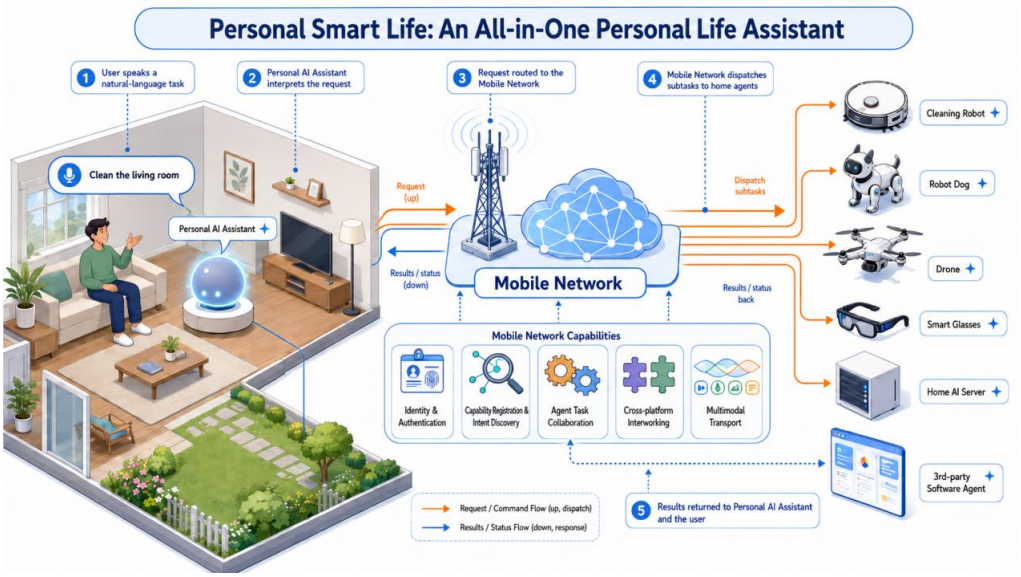

Figure 1 Agents for Personal/Home Scenarios

2) High-End Industrial Manufacturing: Embodied Intelligent Robot Cluster Collaboration

In manufacturing of certain products such as new energy vehicles and high-end equipment, multiple heterogeneous embodied intelligent robots replace traditional production lines to perform complex tasks like battery module handling and flexible assembly. This scenario places high demands on tight collaboration and real-time control of robot clusters. Transport robots, Automated Guided Vehicles (AGVs), network agents, and industrial control platforms potentially have communication roles.

Key communication requirements:

- Highly reliable task collaboration: Support real-time command interaction and synchronization of mechanical and positioning data between robots, with transmission latency ≤ 20ms;
- Dynamic network isolation: Establish dedicated subnets for robot clusters based on production tasks, achieving resource isolation and dedicated assurance within the task domain;
- Device capability interoperability: Support capability discovery and coordinated invocation across robots from different vendors and of different types.

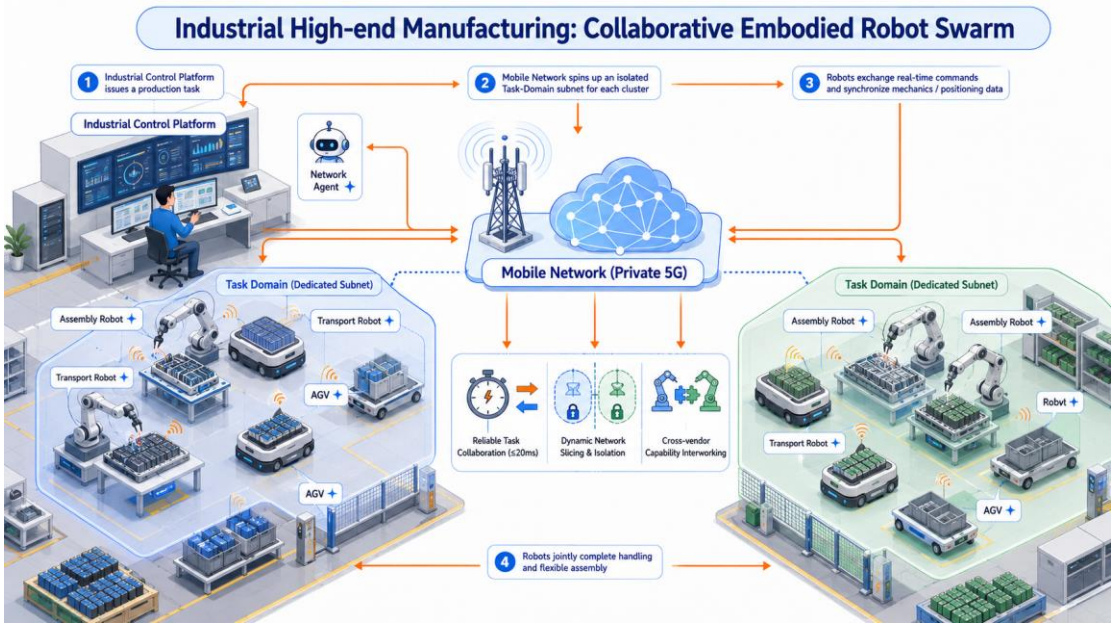

Figure 2 Agents for Industrial Manufacturing Scenarios

3) Public Safety: Wide-Area Agent Patrol and Emergency Response

In outdoor security, campus protection, and emergency rescue scenarios, patrol clusters composed of robot dogs, drones, and other agents achieve wide-area sensing, risk identification, and real-time response, while supporting remote user command and multi-agent relay collaboration. Robot dogs, drones, user terminals, emergency command platforms, and edge computing platforms potentially have communication roles.

Key communication requirements:

- Dynamic addressing for mobile scenarios: Support seamless network handover and routing optimization during agent movement;
- Group-based wide-area collaboration: Support multicast communication and publish-subscribe mechanisms for multiple agents, enabling wide-area synchronization of risk information;

- Highly reliable data transmission: Guarantee lossless transmission of video and sensing data in complex wireless environments, with support for resumable transfers.

Figure 3 Agents for Public Safety Scenarios

4) Network-Native Intelligence: Network Operations Agent Collaboration

Multiple Operations and Maintenance (O&M) agents are deployed within communication networks to automate experience management, traffic optimization, network fault diagnosis, and resource scheduling, which typically include fault diagnosis agents, traffic optimization agents, and Quality of Experience (QoE) assurance agents. Network O&M agents or tools, terminals, network elements, and network management platforms may potentially have communication roles.

Key communication requirements:

- Efficient in-network interaction: Support lightweight interface invocations between agents and network elements, minimizing protocol overhead;
- Trusted data flow: Dynamically authorize agent access to network element data based on task requirements, ensuring network data security;
- Real-time decision synchronization: Support sharing of decision results among multiple O&M agents, achieving global network optimization.

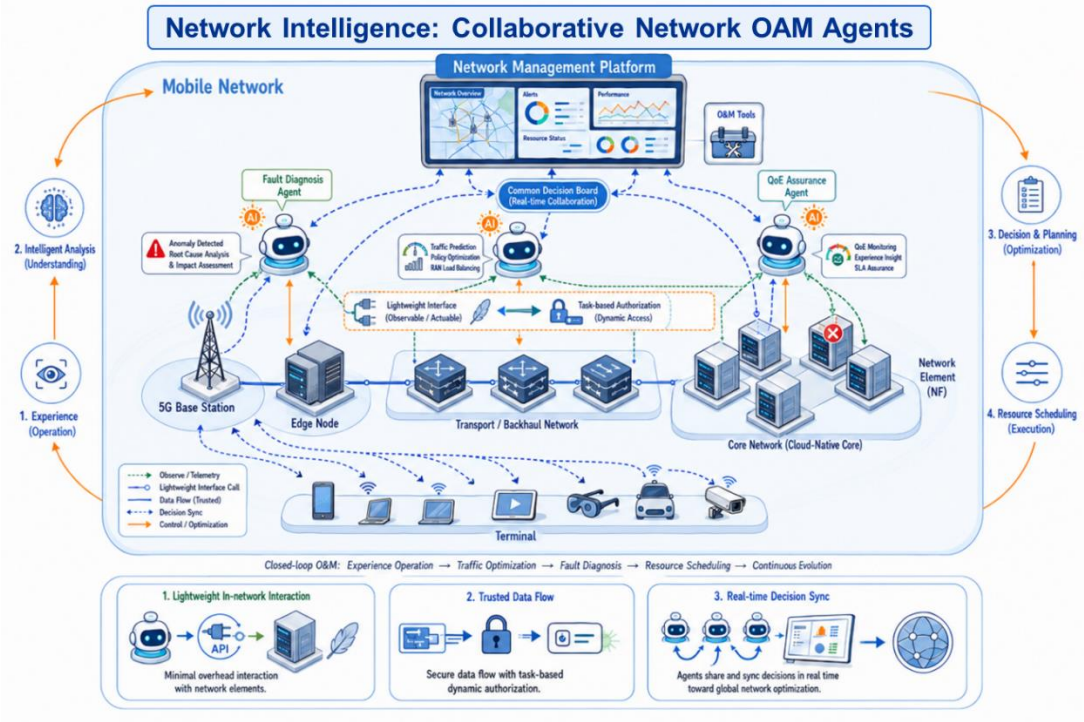

Figure 4

Agents for Network O&M Scenarios

2.2 Industry Progress

2.2.1 Progress in Agent Protocol Standardization

Standardization and technical R&D of agent communication protocols have become a global research hotspot. International and domestic standards organizations including 3rd Generation Partnership Project (3GPP), Internet Engineering Task Force (IETF), and China Communications Standards Association (CCSA), technology companies such as Google, Anthropic, and Cisco, as well as the Agent Network Protocol (ANP) open-source community have all carried out related work in this area.

1) 3GPP: Focusing on AI Agent Support Capabilities for 6G Networks

3GPP has designated AI Agents as one of the essential applications for 6th Generation (6G) mobile communication in 3GPP TR 22.870, which discusses 6G use cases and services with their potential requirements), identifying AI-enhanced key scenarios and positioning agents in the core research dimension of the AI domain. Since 2025, 3GPP has completed a general conceptual definition of AI Agents in SA1 — "an entity that autonomously performs tasks on behalf of users, systems, or applications." Meanwhile, SA2 established the WT#3 topic in the FS_6G_ARC research project under Release 20, focusing on 6G architecture support for AI (including AI Agents and AI frameworks), and proposing two key issues: KI#18 (AI Support for 6G Architecture) and KI#19 (6G Networks for AI). In April 2026, 3GPP CT3#146 meeting agreed the study item on the Protocol for AI in 6G, which was updated in May 3GPP CT3#147 meeting and was approved in June 3GPP CT#112 plenary officially launching discussions on AI (e.g. agent, intent) protocols for 6G with a focus on protocol evolution paths.

2) IETF: Focusing on Agent Protocol Adaptation for Internet of Agents

In May 2025, the first discussion draft on an AI agent communication framework, co-authored by Jonathan Rosenberg and Cullen Jennings, who are core contributors to the Session Initiation Protocol (SIP) and Media over QUIC (MoQ) protocols, attracted widespread community attention. In July of the same year, agent protocol-related side meeting discussions emerged at IETF Meeting 123 in Madrid. In November 2025, a large number of agent communication-related drafts were submitted at IETF Meeting 124 in Montreal, drawing global attention. In March 2026, the first official discussion session was held at IETF Meeting 125 in Shenzhen. A blueprint for research is now taking shape within IETF, structured as one overall framework + multiple specific protocols (e.g., identity, discovery, security, session, routing), centered on scenario-based requirements. Main research directions include:

- Agent communication protocol framework: Defining general requirements for agent communication, characterizing how agents communicate and network with each other, and outlining the overall cross-layer protocol stack for identity registration, capability discovery, authentication and authorization, routing and addressing, and task coordination;
- Agent communication: Including general agent-to-agent protocols (referencing Google's A2A protocol and the ANP community's ANP protocol), as well as agent-to-tool invocation protocols such as Anthropic's MCP protocol;
- Registration and discovery: Agent capability registration and intent-driven capability discovery;
- Identity and security: Definition and management of agent identity, cross-ecosystem identity mutual recognition, agent authentication and authorization;
- Session and routing: Agent task sessions, context management, multi-modal data transmission, and dynamic routing optimization for mobility.

IETF's exploratory work on the technical elements of agent communication has started, and we can see how and when IETF will formally pursue agent work..

2.2.2 Agent Communication Protocol Implementations Continue to Emerge

Domestic and international enterprises have released multiple open-source agent communication protocols and frameworks, covering use cases ranging from internal enterprise collaboration to cross-enterprise agent and tool invocations. Representative protocols include A2A, MCP, ANP, Agent Interconnection Protocol (AIP) and so on. The core characteristics and applicable scenarios of each protocol are shown in the table below:

Table 1 Core Characteristics and Applicable Scenarios of Agent Protocols

Protocol / Framework	Issuer	Core Positioning	Core Features	Applicable Scenarios
Agent2Agent (A2A)	Google / Linux Foundation	Agent-to-agent communication and interoperability protocol	Supports capability discovery, task management, asynchronous collaboration; based on HTTP(S); compatible with JSON-RPC 2.0 / gRPC	Multi-agent collaboration within enterprises; small-scale agent networking
Model Context Protocol (MCP)	Anthropic	Connection protocol between large models and external resources	Based on JSON-RPC 2.0; supports Stdio/SSE transport; enables efficient interaction	Tool invocation and data retrieval for large model agents

Protocol / Framework	Issuer	Core Positioning	Core Features	Applicable Scenarios
			between large models and tools/APIs	
Agent Network Protocol (ANP)	ANP Open Source Community	Decentralized identity, discovery, instant messaging, and payment protocol for interoperable AI agents	Automatic agent discovery; autonomous task collaboration; secure cross-domain interoperability; layered architecture design; fully autonomous operation	Agent collaboration networks; multi-agent systems; decentralized AI applications; intelligent data exchange; automated service orchestration; cross-platform agent interoperability
Agent Interconnection Protocol (AIP)	Co-led by the China Electronics Standardization Institute and Beijing University of Posts and Telecommunications (open-source community hosted by the OpenAtom Open Source Foundation)	Agent interconnection protocol based on the 'Artificial Intelligence – Agent Interconnection' series of national standards; adopts a multi-autonomous-domain architecture to build an agent interconnection ecosystem compliant with national standards	Includes six core modules: identity code, identity management, agent description, agent discovery, agent interaction, and tool invocation; provides verifiable digital identity and standardized capability descriptions; introduces "autonomous domains"; compatible with A2A/MCP; supports message queue group communication	Cross-vendor agent interconnection and group collaboration in open network environments, such as mobile terminal agent interconnection and robot agent interconnection — scenarios requiring trusted registration, identity management, and capability discovery

2.3 Core Challenges

Existing agent protocols primarily support non-real-time data interaction in client/server architectures. Only a few protocols are adapted to the characteristics of mobile communication networks, including wide-area mobility, heterogeneous access, high reliability, and security control, and further enhancement is still needed to meet the requirements of cross-ecosystem and cross-domain agent collaboration. The core challenges of existing protocols are concentrated in the following six areas:

1) Cross-Domain Identity Mutual Recognition Is Difficult; Dynamic Authorization Mechanisms Are Absent

Agent collaboration scenarios involve user domains, operator network domains, and third-party platform domains. There is no unified identity trust framework across these domains, making it difficult for agents to achieve cross-domain identity mutual recognition. At the same time, traditional static authorization mechanisms are ill-suited to the task-oriented and dynamic nature of agent collaboration. There is an urgent need for task-based least-privilege dynamic authorization mechanisms, which can grant agents temporary capability invocation and data access permissions based on task requirements, and automatically revoking them upon task completion, to protect data privacy and security.

2) Cross-Ecosystem Capability Discovery Is Difficult; Heterogeneous Agent Silos Are Widespread

Agent forms are highly heterogeneous, encompassing embodied agents (robots, drones), wearable agents (AI glasses, smartphones), and virtual agents (digital humans, large model assistants). Agents from different ecosystems adopt varying capability descriptions, communication protocols, and data formats. The technical systems of the smartphone ecosystem (Android/HarmonyOS), the OTT (Over-The-Top) ecosystem (Microsoft/ByteDance), and the embodied ecosystem (DJI/Zhiyuan) are mutually independent. Currently, there is a lack of unified capability description specifications and cross-domain discovery mechanisms among heterogeneous cross-ecosystem agents, making it difficult to achieve capability discovery and task collaboration between agents, and resulting in "agent silos."

Most existing agent communication protocols remain at the level of "message interaction", which is oriented toward request-response type of data exchange, and lack full lifecycle task management (creation, allocation, execution, feedback, and termination) and multi-principal collaboration mechanisms, making it difficult to support master-slave and peer-to-peer collaboration for complex tasks. At the same time, protocols generally lack the ability to parse, disambiguate, and standardize unstructured intents such as natural language, making it impossible to precisely map user/network/business intents to agent tasks, thereby constraining the automation and intelligence level of agent collaboration.

4) Multi-Modal Differentiated Transmission Is Difficult; Mobile Addressing and Routing Are Mismatched

Agent collaboration relies on interaction across multiple modalities including text, audio, images, video, sensing data, and control commands. Different modalities impose significantly different transmission requirements. For example, real-time and non-real-time communication imply different specifications, control commands require low latency ($\leq$ 20ms), video data requires high bandwidth, and sensing data requires high reliability. Existing protocols lack unified encapsulation and differentiated transmission assurance mechanisms for multi-modal data, making it difficult to achieve synchronized transmission and independent Quality of Service (QoS) scheduling for multiple modal streams within a single session. Additionally, mobility is a core characteristic of mobile communication network scenarios. Agents such as patrol robots and drones face issues related with network access point handover and changing wireless environments during their mission. Existing protocols lack dynamic addressing and routing optimization mechanisms for mobile agents, making it impossible to guarantee highly reliable forwarding of task data or to proactively plan allocation and management of network resources based on mobility trajectories.

5) Protocol Adaptation and Interoperability Are Difficult; Ecosystem Fragmentation Is Intensifying

Since 2023, the industry has released over 20 agent communication protocols. Agents from different ecosystems adopt varying communication protocols and data formats, making the protocol ecosystem highly fragmented. At the same time, existing protocols are mostly designed for IT application scenarios and are insufficiently adapted to the network element interfaces and protocol specifications of telecom networks. When agents collaborate across ecosystems and domains, there is a lack of unified abstract interfaces and protocol adaptation mechanisms, making it difficult to shield the differences in underlying networks and protocols. These circumstances collectively result in high costs for interconnection and large-scale retrofitting.

6) Telecom-Grade Security Management Is Difficult; Privacy Protection Capabilities Are Insufficient

Agent collaboration scenarios on mobile communication networks involve personal privacy, industrial data, and core network data, imposing telecom-grade requirements on security and privacy protection. The security mechanisms of existing protocols are mostly designed for internet scenarios and lack end-to-end encryption, data desensitization, and behavior control capabilities, making it difficult to guard against security risks such as agent identity spoofing, privilege abuse, and data leakage, and to meet the "controllable and manageable" requirements of telecom networks.

3 Key Principles for Protocol design

3.1 Key Principles

The design of agent protocols for mobile communication networks should be grounded in the collaboration needs of agents and the technical characteristics of telecom networks, guided by the core philosophy of having "compatibility and inclusiveness, layered decoupling, dynamic adaptation, and security and trustworthiness" as the foundational principles for protocol design and development.

1) Compatibility and Inclusiveness

The protocol system should be compatible with existing mainstream industry agent protocols (such as A2A and MCP) and traditional communication protocols (such as HTTP, and SBI), achieving "openness at both ends": one end interfacing with the network element interfaces and protocol specifications of telecom networks, and the other compatible with the agent protocol ecosystems of the internet and industrial sectors, avoiding technology stack reconstruction and ecosystem fragmentation. At the same time, it should reuse existing achievements of standards organizations such as IETF and 3GPP as much as possible to reduce redundant R&D effort.

2) Layered Decoupling

The protocol system adopts a layered architecture, decoupling core capabilities such as identity management and identification, capability discovery, task coordination, transmission and networking, and security, authentication and privacy protection into mutually independent functional layers that interact through standardized interfaces. Layered decoupling enables independent evolution and flexible extension of each functional layer, adapts to protocol tailoring requirements for different scenarios, and reduces the complexity of technical development and deployment.

3) Dynamic Adaptation

The protocol should enable dynamic adjustment of transmission parameters, networking modes, and authorization policies based on agent type, task requirements, and network conditions. For example, dynamically updating routing and addressing information for mobile agents, dynamically allocating QoS resources for multi-modal data, dynamically adjusting agent capability invocation permissions based on task phase, achieving "on-demand adaptation and dynamic optimization" are desirable properties.

4) Security and Trustworthiness

Security and privacy protection should be integrated into the entire process of protocol design, building an end-to-end security system covering identity authentication, data transmission, and task execution. The protocol must support universal trusted identity management for agents, task-based least-privilege dynamic authorization, and end-to-end data encryption and privacy enhancement, ensuring trustworthy identity, secure transmission, and controlled data throughout agent communication, and meeting the security management requirements of telecom networks.

3.2 Overall Design of Agent Protocols

Based on the key principle of "layered decoupling," a core capability architecture for agent communication protocols has been designed. The protocol relies on the underlying communication networks such as 5G, 6G, and fixed-line networks, and are supported by a security protection that provides end-to-end security assurance throughout all processes.

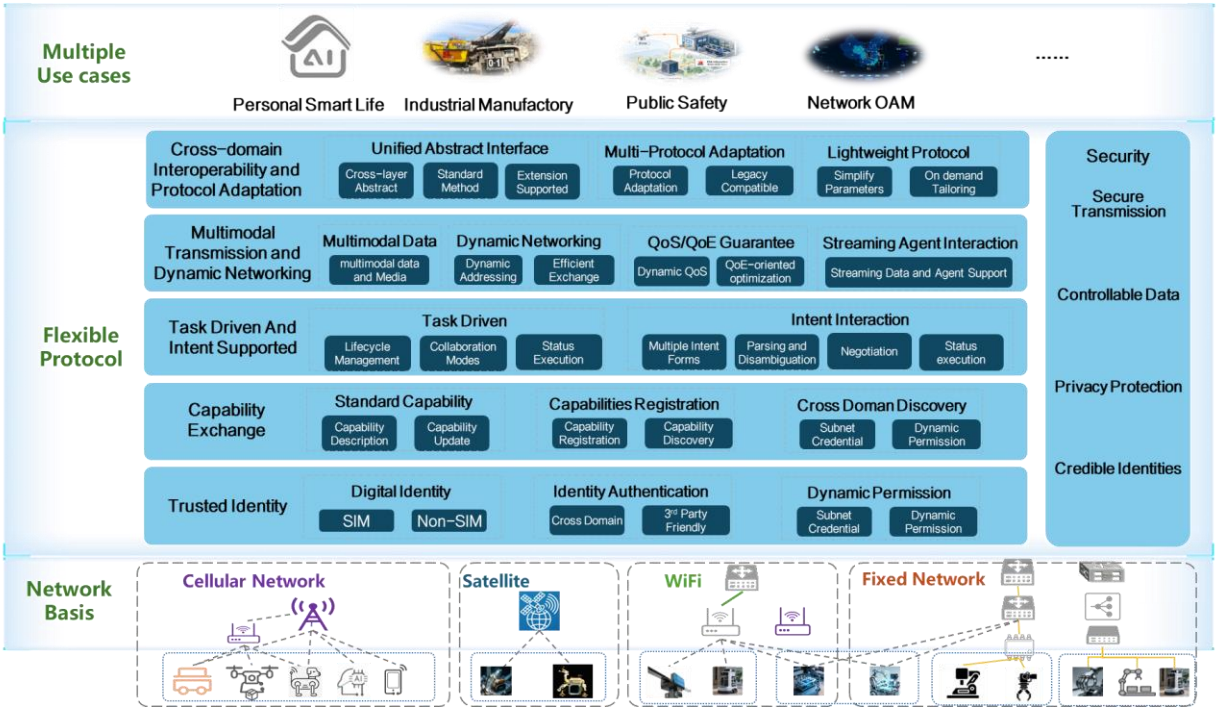

Figure 5 Overall Architecture of Agent Protocols

4 Key Capabilities and Mechanism

4.1 Identity and Trust Mechanisms

Identity management and identification are the foundation of agent communication. The protocol must establish a globally unified, cross-domain mutually recognized, and dynamically managed digital identity system for agents, achieving trustworthy identities and controllable permissions, which fulfill the core principle of "security and trustworthiness."

The agent digital identity system should be built around the core elements of "identifier + attributes + credentials," encompassing an identity management module, a third-party attribute management module, a subnet attribute credential management module, an agent behavior security management and control module, and a cross-domain mutual trust module. It should support unified access for SIM and non-SIM agents, be compatible with frontier technologies such as Decentralized Identifier (DID) and Verifiable Credential (VC), and provide a trusted identity foundation for cross-domain agent communication.

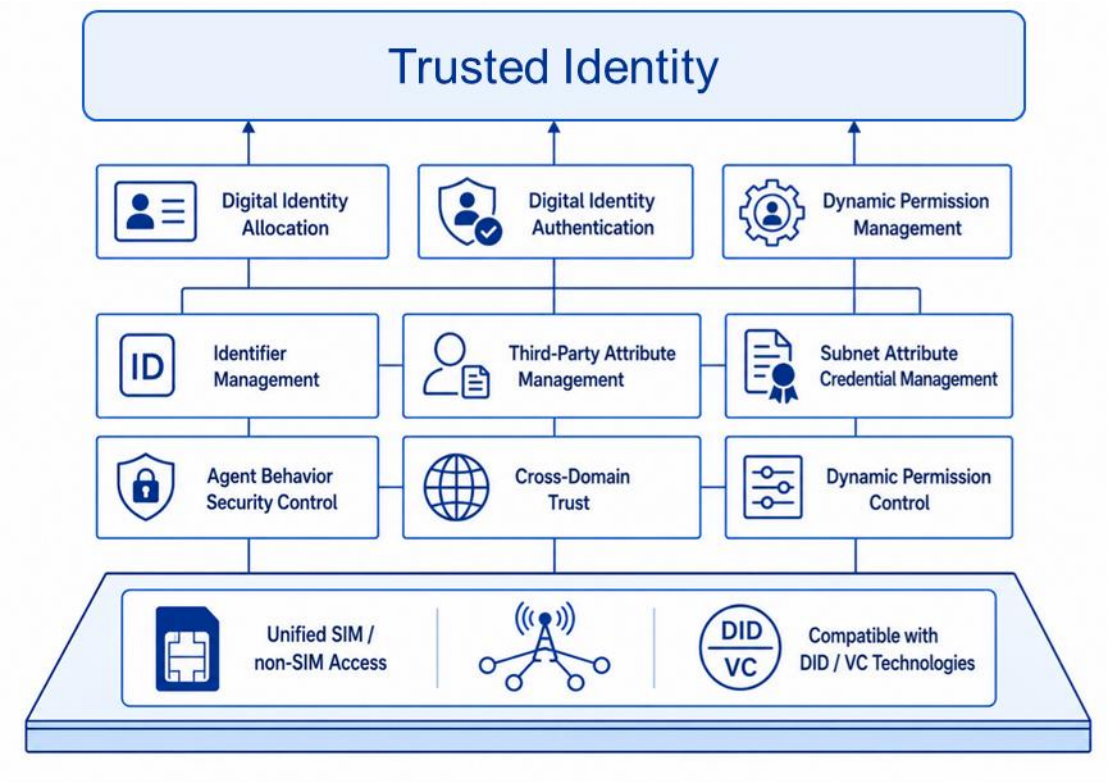

Figure 6 Identity and Trust Mechanism

1) Digital Identity Assignment

The agent protocol should support the use of unique, globally recognizable digital identities (Digital IDs) for all agents accessing mobile communication networks (including SIM and non-SIM agents). Identifiers should be capable of indicating the agent type, affiliated ecosystem, capability summary, and affiliation relationships, and should support standardized parsing and cross-domain recognition. Agent identifiers should be linkable to SIM permanent identifiers to support digital identity derivation for personally affiliated agents (such as AI glasses and home robots), enabling identity association and management for "one person, multiple agents". The agent protocol should also support full lifecycle management of agent

digital identities, including registration, assignment, updating, cancellation, and traceability, which can ensure controllable and manageable identity information.

2) Digital Identity Authentication

The agent protocol should support multiple authentication methods for agent identity identifiers, adaptable to the security requirements of different scenarios, enabling mutual authentication between agents and interacting entities to prevent identity spoofing. The agent protocol should support cross-domain identity mutual trust mechanisms, compatible with identity systems from OTT ecosystems and industrial ecosystems (such as DID/VC), enabling identity mutual recognition across user domains, operator network domains, and third-party platform domains. The agent protocol should also support privacy protection to meet agent identity privacy requirements in sensitive identity information scenarios.

3) Dynamic Permission Management

The agent protocol should support fine-grained, task-based permission management, dynamically allocating capability invocation and data access permissions based on agent task requirements and identity attributes, granting only the minimum permissions necessary to complete the task, and avoiding over-authorization of permissions.

4.2 Capability Registration and Discovery Mechanisms

Capability registration and discovery are prerequisites for multi-agent collaboration. The agent protocol must build a standardized, cross-domain, and efficient agent capability management mechanism to achieve standardized capability description, dynamic publication, and precise discovery, which can resolve the "agent silo" problem. The agent protocol should support standardized capability description, capability registration and synchronization, and cross-domain capability discovery.

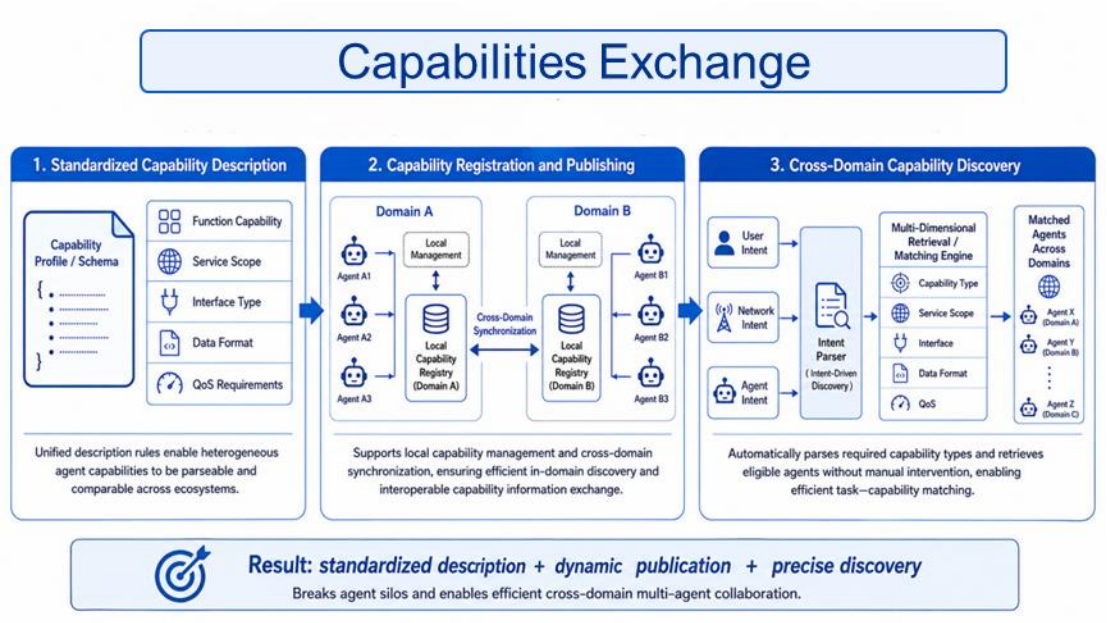

Figure 7 Capability Registration and Discovery Mechanism

1) Standardized Capability Description

The agent protocol should support standardized description specifications for agent capabilities, providing

unified descriptions of agents' functional capabilities, service scope, interface types, data formats, and QoS requirements, enabling parsable and comparable representations of capabilities across different ecosystem agents. The agent protocol should also support hierarchical and tiered capability descriptions, categorizing agent capabilities into core capabilities and extended capabilities by capability level, facilitating precise matching by other agents based on task requirements. Furthermore, the agent protocol should support dynamic updates to capability descriptions. When an agent's capabilities change, it can update the capability description information in real time at the capability registry, ensuring the timeliness of capability information.

2) Capability Registration and Synchronization

The agent protocol should support local management and cross-domain synchronization of agent capabilities, ensuring efficient intra-domain capability discovery and enabling cross-domain capability information interoperability. The agent protocol should also be compatible with existing network and service discovery mechanisms, supporting parsing and querying of agent capability information to reduce deployment complexity.

3) Cross-Domain Capability Discovery

The agent protocol should support multi-dimensional capability retrieval for efficient matching between agents and task requirements. The agent protocol shall also support intent-driven capability discovery, enabling automatic parsing of required capability types based on user/network/agent intent and retrieval of matching agents without manual intervention; and achieve cross-ecosystem and cross-domain capability discovery, breaking down the boundaries of smartphone, application, embodied intelligence, and other ecosystems, as well as the geographical boundaries of operator network domains, application provider domains, and service consumer domains, supporting wide-area agent capability retrieval.

4.3 Task-Driven and Intent Interaction

Task-driven operation is the core distinction between agent protocols and traditional messaging protocols. The protocol must achieve an upgrade from "message interaction" to "task collaboration," while supporting efficient intent interaction to precisely translate user/network/business intents into agent tasks.

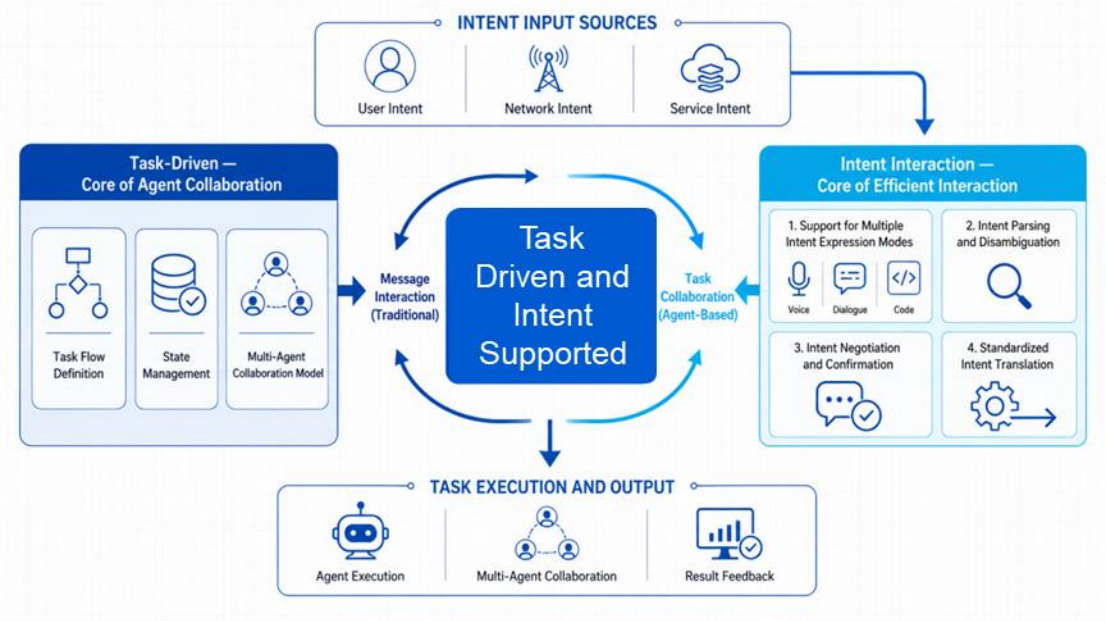

Figure 8 Task-Driven and Intent Interaction Mechanism

1) Task-Driven

Task-driven operation enables full lifecycle management and multi-principal collaboration for agent tasks, and is the core of agent collaboration. The agent protocol must define clear task processes, state management, and collaboration modes.

- The agent protocol should support full lifecycle task management, meeting the core interaction management requirements for task creation, allocation, execution, feedback, and termination throughout the entire lifecycle, achieving standardized task processes.
- The agent protocol should support at least two task collaboration modes in the form of client-server and peer-to-peer architectures. And the protocol should adapt to different task complexities and scenario requirements.
- The agent protocol should support real-time synchronization of task execution states, using standardized interaction formats to enable compressed data transmission and incremental synchronization, reducing transmission overhead and improving interaction efficiency. It should also support handling of exception types (such as network interruption, agent failure, and task timeout) to ensure that the master agent/collaborators have a comprehensive view of the global task state.

2) Intent Interaction

The intent interaction protocol enables efficient intent exchange between users/networks/businesses and agents, as well as between agents, supporting the parsing and transformation of unstructured intents such as natural language. The agent protocol should support the following four mechanisms:

- Multi-intent expression support: Compatible with multiple intent expression methods including natural language, structured commands, and voice, to meet the interaction requirements of different scenarios, such as natural language for individual users and structured commands for industrial scenarios;
- Intent parsing and disambiguation: Built-in intent parsing algorithms capable of parsing and disambiguating vague or unclear intents that are combined with contextual information and agent capabilities to accurately understand the true needs of users/networks/businesses;
- Intent negotiation and confirmation mechanism: When intents are unclear or multiple execution plans exist, the protocol supports intent negotiation between agents and interacting parties, offering multiple execution plans for selection, and receiving confirmation before converting the plan into task instructions;
- Standardized intent translation: Converting parsed intents into standardized, machine-recognizable instructions and mapping them to agent task requirements, achieving precise translation from intent to task and ensuring the accuracy of task execution.

4.4 Multi-Modal Transmission and Dynamic Networking

The transport layer is the network base for agent communication. The protocol must shield the complexity of underlying networks, providing multi-modal adaptation, dynamic networking, highly reliable, and low-latency transport services, adjusting to the mobility and heterogeneity characteristics of mobile communication networks. The core technical requirements include four aspects: multi-modal data and differentiated transmission adaptation, dynamic networking and routing, QoS/QoE assurance, and streaming interaction support.

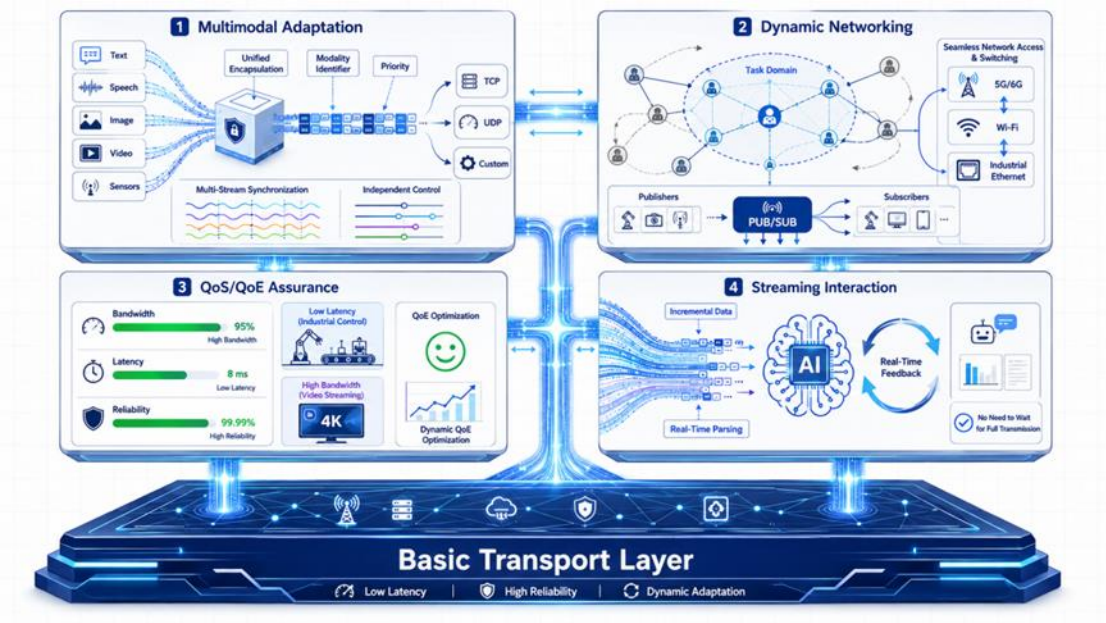

Figure 9 Multi-Modal Transmission and Dynamic Networking Mechanism

1) Multi-Modal Data and Differentiated Transmission Adaptation

Multi-modal data unified encapsulation: Defines unified encapsulation formats for text, audio, images, video, sensing data, real-time audio streams, real-time video streams, real-time data streams, control commands, and other multi-modal data types. Different modal data are encapsulated into standardized data packets, carrying metadata such as modal identifiers, transmission priorities, and QoS requirements to facilitate differentiated scheduling by the network.

The agent protocol should support adapting optimal transport protocols for different modal data to maximize transmission performance for each modality, while also supporting synchronized transmission and independent control of multiple modal streams within a single session to ensure temporal synchronization of multi-modal data, such as synchronization between a robot's video feed and control commands, avoiding desynchronization between video and commands.

2) Dynamic Networking and Routing

The agent protocol should support establishing task domains for agent clusters based on task requirements, achieving resource isolation, dedicated assurance, and efficient communication within the task domain. The agent protocol should support dynamic addressing and routing for mobile agents, meeting the requirements for dynamic updates of agent location and mobility trajectory, optimizing routing paths, and ensuring lossless data forwarding as the agent moves. The agent protocol should be compatible with multiple network access types, supporting agent access via 5G/6G, Wi-Fi, industrial Ethernet, and other networks, and further enabling seamless handover across multiple networks. The agent protocol should support efficient group communication mechanisms, including multicast and publish-subscribe (PUB/SUB) mechanisms, for efficient multi-agent data distribution, reducing network bandwidth overhead, suitable for multi-principal collaboration scenarios such as patrol clusters and robot clusters.

3) QoS/QoE Assurance

The agent protocol should support task-priority-based QoS negotiation, enabling dynamic negotiation of

QoS parameters between agents and the network, allocating resources based on task priority and modal data transmission demands that are mapped to bandwidth, latency, packet loss rate, and other QoS requirements. For example, allocating low-latency, highly reliable QoS resources for industrial control tasks and high-bandwidth QoS resources for general video tasks. The agent protocol should also support experience-centric QoE assurance: for individual user scenarios, the protocol supports QoE sensing and optimization, dynamically adjusting transmission strategies based on user experience feedback and network conditions to improve subjective user experience.

4) Streaming Agent Interaction Support

To address the streaming interaction requirements of large model agents and real-time inference agents, the agent protocol should support continuous transmission and real-time processing of streaming data, enabling reception of incremental streaming data with real-time parsing and feedback without waiting for complete data transmission. The protocol should improve the real-time performance and efficiency of agent interaction.

4.5 Cross-Domain Interoperability and Protocol Adaptation

The heterogeneity of agents and the complexity of networks require protocols to have unified interfaces and flexible adaptation capabilities, shielding agents from the complexity of underlying networks and protocols, providing simple and efficient interaction interfaces, while being compatible with existing industry protocols and telecom network interfaces, realizing the core philosophy of "compatibility and inclusiveness". The core technical requirements include three aspects: unified abstract interfaces, multi-protocol compatibility and adaptation, and lightweight interface design.

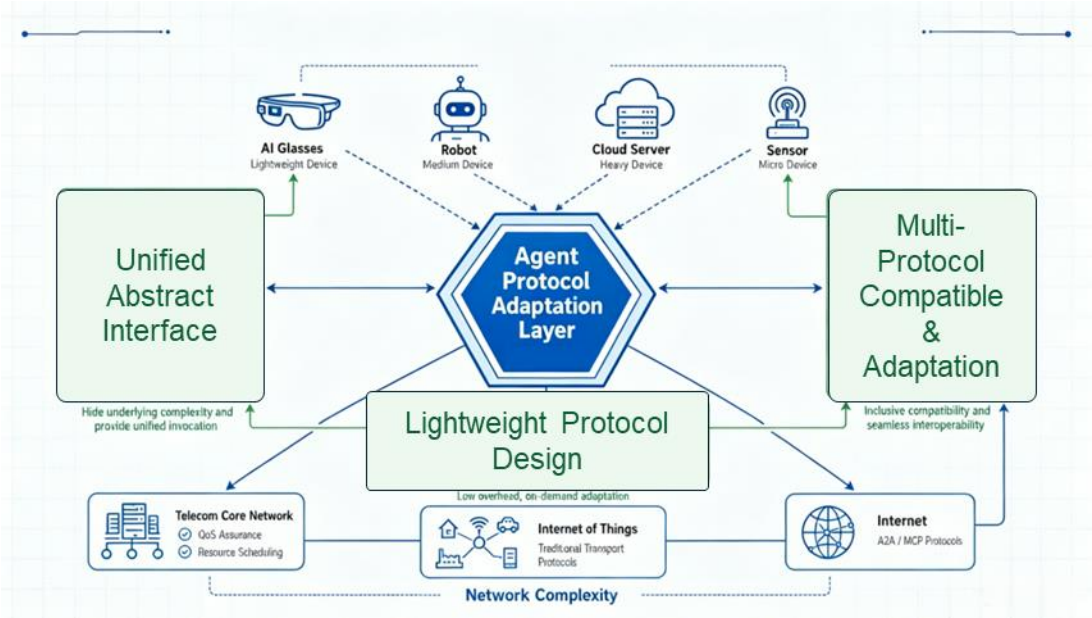

Figure 10 Cross-Domain Interoperability and Protocol Adaptation Mechanism

1) Unified Abstract Interfaces

The agent protocol should support cross-layer unified abstract interfaces, encapsulating core capabilities such as identity management and identification, capability discovery, task coordination, transmission and networking, and security, authentication and privacy protection into standardized interfaces. Agents only need to invoke the unified interfaces to implement all communication functions, without needing to

concern themselves with the underlying technical details. The agent protocol should support standardized interface invocations, including interface parameters, return values, invocation methods, and exception handling, enabling unified invocation of interfaces by different agents and platforms to improve development and integration efficiency. The agent protocol should also support flexible interface extension, with reserved extension positions that allow new interface functions to be added flexibly in response to new scenario requirements and technological developments, enabling smooth protocol evolution.

2) Multi-Protocol Compatibility and Adaptation

The agent protocol should support broad compatibility with existing industry agent protocols, meeting interoperability requirements with mainstream protocols such as A2A and MCP, enabling interconnection between different protocols and this protocol through protocol adaptation, without requiring large-scale retrofitting of existing agents. The agent protocol should also be compatible with traditional communication protocols and standard implementation mechanisms, including transport, capability discovery, and identity management mechanisms, to improve protocol deployment feasibility. The agent protocol should additionally support interoperability with telecom networks, enabling agents to invoke core network capabilities such as resource scheduling, QoS assurance, and identity management.

3) Lightweight Interface Design

To address the limited computing and communication resource constraints of lightweight agents (such as AI glasses, sensors, and small robots), the agent protocol should support lightweight interfaces, simplifying interface parameters and invocation processes to reduce interface computing and communication overhead. The agent protocol should also support on-demand interface tailoring and modular assembly, enabling customization to fit different devices based on agent type and scenario requirements. The agent protocol should support the use of efficient interface data formats to reduce data transmission overhead and improve the efficiency of interface invocations.

4.6 Security, Authentication and Privacy Protection

Security is a core requirement for agent communication in mobile communication networks. The agent protocol must build an end-to-end, full-process security protection system, achieving trustworthy identity, secure transmission, controlled data, and privacy protection, meeting the "controllable and manageable" requirements of telecom networks.

In telecom networks, agents may exist within operator networks or on the device side. Agent communication scenarios may include receiving intents from terminals, understanding them as corresponding tasks, and further having other agents or APIs execute subsequent operations for agents within operator networks, whereas for device-side agents, sending user intents or tasks to the network based on user requirements will be required. Additionally, there are third-party platform agents that can invoke or be invoked by agents within operator networks to collaboratively complete tasks.

From a security domain perspective, agent interaction involves three types of domains: user domain, operator network domain, and third-party platform domain. Since there is a lack of trust foundations between domains, the authentication mechanisms between inter-domain entities must be considered first. Furthermore, privilege abuse may occur in communications between inter-domain entities, so changes to authorization mechanisms between inter-domain entities must also be considered. Beyond inter-domain entity authentication and authorization, interactions between intra-domain entities also require consideration of authentication and authorization mechanisms, so authentication and authorization changes must also be considered when intra-domain agents interact with surrounding entities.

5 Outlook

The research and development for agent protocols, and their subsequent deployment, is a gradual and progressive process that cannot achieve universal agent protocol interoperability in a single step. In next-generation mobile communication networks, all types of new terminal devices and network infrastructure are accelerating their evolution toward agent-based models. Large-scale access and wide-area, cross-domain, cross-ecosystem collaborative operations of diverse agent types are becoming key capabilities for supporting complex future service scenarios. As the foundational capability enabling efficient and secure agent collaboration, agent communication protocols are attracting increasingly widespread attention across the industry.

The rapid development of agents is reshaping the form and boundaries of network services, and unified, efficient agent communication protocols will become the core driving force for unlocking the potential of agents. Looking to the future, through agent communication protocols, operators are expected to drive the transformation of networks from "pipeline connections" to "intelligent service hubs," achieving a leap from the Internet of Everything to the interconnection of billions of agents.

At present, new agent communication protocols continue to emerge in the industry, and there is an urgent need for operators to work with industry partners to support the evolution of agent communication protocols for mobile communication networks. To this end, the following proposal is put forward: jointly with equipment vendors, vertical industries, research institutions, and operators, guided by scenario-specific requirements, collaboratively refine the core application specifications for inter-agent communication, promote standardization and interoperability of protocols, prevent fragmentation of protocols and technology stacks, and make agent communication protocols the bridge and cornerstone of agent technology innovation and industrial deployment.

Annex: Contributors

China Mobile Research Institute
Turk Telekom
ANP Open Source Community
CATT
China Southern Power Grid
CSG Digital Grid Group Information & Communication Technology
Cygnusemi
DEEP Robotics
Digit Technology
Hongdian
Huawei
Humanoid Robotics Association Switzerland
Midea Group Co., Ltd.
Nokia
OPPO
Oray
Rokid
Shanghai MScape Technology Co., Ltd.
State Grid Shandong Electric Power Company, Information & Communication Company
State Key Laboratory Of High-end Heavy-load Roborts
TD Tech
UBTECH ROBOTICS CORP LTD
Vivo
ZTE

Annex: Acronyms and Abbreviations

Abbreviation	Full Name
3GPP	3rd Generation Partnership Project
5G	5th Generation Mobile Communication
6G	6th Generation Mobile Communication
A2A	Agent-to-Agent (Agent2Agent)
AGV	Automated Guided Vehicle
AI	Artificial Intelligence
AIP	Agent Interconnection Protocol
ANP	Agent Network Protocol
API	Application Programming Interface
CCSA	China Communications Standards Association
DID	Decentralized Identifier
Digital ID	Digital Identity
HTTP	Hypertext Transfer Protocol
ICT	Information and Communications Technology
IETF	Internet Engineering Task Force
MCP	Model Context Protocol
MoQ	Media over QUIC
OTT	Over The Top
QoE	Quality of Experience
QoS	Quality of Service
SBI	Service Based Interface
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
VC	Verifiable Credential