

ArXiv Papers:

1. MCP Bridge: A Lightweight, LLM-Agnostic RESTful Proxy for Model Context Protocol Servers

Description: This paper introduces MCP Bridge, a RESTful proxy that enhances security and compatibility across platforms by connecting to multiple MCP servers.

Link: [Read the paper](#)

2. MCP Safety Audit: LLMs with the Model Context Protocol Allow Major Security Exploits

Description: The paper discusses security risks associated with MCP and introduces MCPSafetyScanner, a tool for auditing the security of MCP servers.

Link: [Read the paper](#)

3. UMC: A Unified Bandwidth-efficient and Multi-resolution based Collaborative Perception Framework

Description: This study proposes a framework for multi-agent collaborative perception, optimizing communication and collaboration processes.

Link: [Read the paper](#)

4. Autono: A ReAct-Based Highly Robust Autonomous Agent Framework

Description: The paper introduces a robust agent framework that enhances task execution through adaptive decision-making and multi-agent collaboration using the MCP protocol.

Link: [Read the paper](#)

5. MCP: Learning Composable Hierarchical Control with Multiplicative Compositional Policies

Description: This research presents multiplicative compositional policies (MCP) for learning reusable motor skills that can be integrated to create complex behaviors.

Link: [Read the paper](#)

Other Sources:

1. Model Context Protocol (MCP): Landscape, Security Threats, and Future Directions

Description: A comprehensive overview of the MCP protocol, discussing its components and security implications.

Link: [Read more](#)

2. Uncovering MCP Security: Threat Mapping and Vulnerability Analysis

Description: A white paper analyzing security threats associated with MCP and proposing an architecture for secure execution.

Link: [Read more](#)

3. Introducing the Model Context Protocol | Anthropic

Description: An introduction to the MCP and its applications in connecting AI models with external systems.

Link: [Read more](#)

4. Announcing the Agent2Agent Protocol (A2A) - Google Developers Blog

Description: This blog discusses A2A, a protocol that complements MCP, aimed at improving multi-agent system functionalities.

Link: [Read more](#)