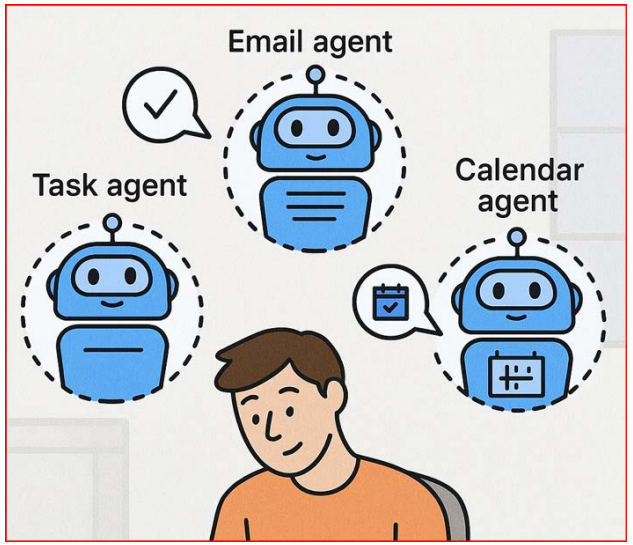
Internet of AI Agents



Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this class lecture are available at:

http://www.cse.wustl.edu/~jain/CSE5700-25/

Student Questions

©2025 Raj Jain



Overview

1. What are AI Agents?
2. Why Internet of AI Agents?
3. Protocols for Internet of AI Agents

Student Questions

©2025 Raj Jain

Agentic AI

- **Agents**:
  - Independently or semi-autonomously performing tasks on behalf of a client, e.g., Insurance Agent, Real Estate Agent
  - One who is authorized to act for or in the place of another, e.g., Artists' agents, federal agents, consular
- **Agentic**: Adjective
  - Capable of achieving outcomes independently
  - Just doesn't react to instructions. It takes initiative, sets its own goals and plans
- **Agentic AI**: Programs that can make decisions, take actions, solve problems, reason, etc., on their own. This is beyond simple chatbots that respond to your queries.
  Example: Resolve a customer service issue or issue a refund without any human oversight.

Ref: Merriam-Webster Dictionary

©2025 Raj Jain

Student Questions

The Evolution and Vision of Agentic AI

- 1970s: Autonomous, asynchronous, message-driven computation
- 1990s: Distributed AI
- 2025: Billions of collaborative agents with machine-scale cognition, action, and cooperation

Student Questions

©2025 Raj Jain

Internet of AI Agents

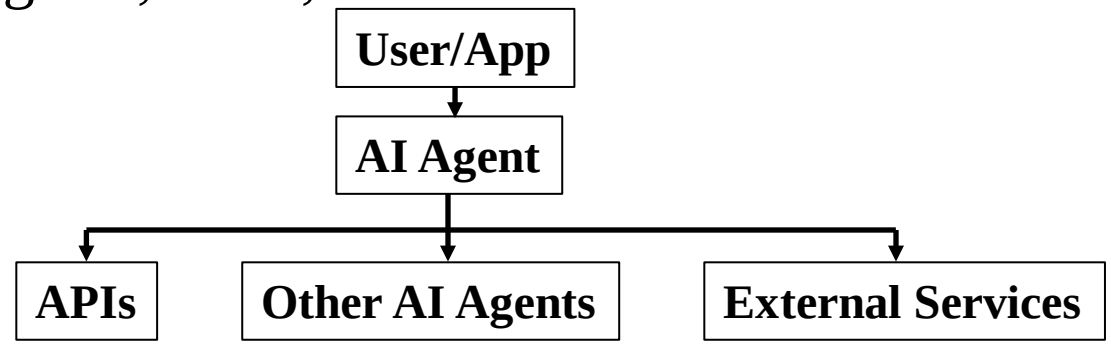
- A distributed Network of autonomous or semi-autonomous software entities powered by AI
- May leverage:
  - Large Language Models (LLMs)
  - Vision models
  - Domain-specific algorithms
- These entities communicate and coordinate to achieve complex goals.
- Can also integrate external tools and systems over the Internet
- Past AI systems were reactive: responding to commands
  AI agents can proactively plan, execute, and adapt multistep tasks autonomously.

Student Questions

©2025 Raj Jain

Fundamental Capabilities of AI Agents

1. **Perception**: Sense environment via sensors, human interaction, or data streams
2. **Reasoning**: Plan, reason, and decompose tasks
3. **Actuation**: Execute tasks by calling APIs, issuing commands, manipulating data, or controlling physical devices
4. **Learning and Adaptation**: Continuously improve via feedback, reinforcement learning, or observations
5. **Communications**: Exchange Information and coordinate with other agents, users, or services



Student Questions

©2025 Raj Jain

Multi-Agent Architectures

- **Single Agent Systems**
- **Multi-Agent Systems (MAS):** Multiple agents collaborate either hierarchically (vertically), peer-to-peer (horizontally), or hybrid
- **Orchestration Patterns:**
  - **Sequential**: Agents act in a defined order (pipeline)
  - **Concurrent**: Agents act in parallel, combining findings (ensemble reasoning)
  - **Group Chat**: Shared thread for negotiation, validation
  - **Handoff**: Dynamic transfer depending on domain expertise required
  - **Magentic**: Open-ended, agent-led task and team formation with evolving task ledgers

Student Questions

- In the handoff pattern, how do we stop two agents with similar skills from bouncing a task back and forth instead of finishing it?

Similar to hop counts in IP.

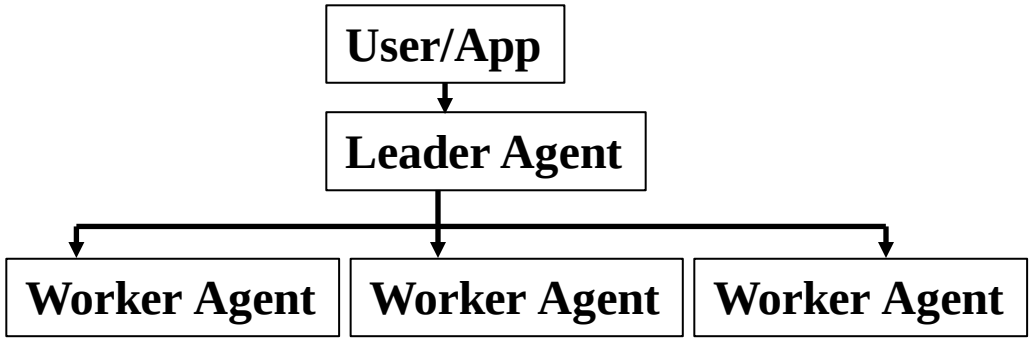
- In the concurrent (ensemble) pattern, when agents give conflicting answers, how should the system pick a final result without adding a lot of delay?

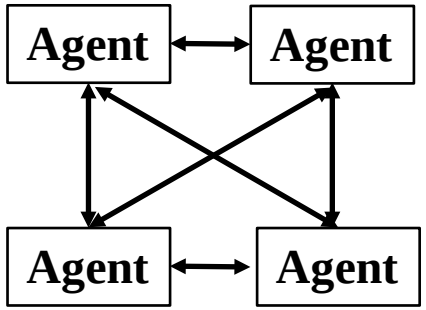
There are ways to find consensus among a population with differing opinions.

©2025 Raj Jain

Topologies: Pros and Cons

- **Centralized (Vertical):** Borrowed from human organization. A leader agent oversees subtasks. Streamlined but bottleneck/failure-prone.
- **Peer-to-Peer (Horizontal):** Agents work as equals. Direct messaging. Robust/scalable. May be slow due to coordination **challenges.**
- **Hybrid**: Combines the above two
- **Dynamic/adaptive**: Graph-based architecture designed using neural networks to optimize agent links and minimize redundancy while maximizing performance.





Student Questions

©2025 Raj Jain

Agent Communication and Coordination Mechanisms

- **Explicit Communication**: Message passing, commands, requests
- **Implicit Communication**: Signals indirectly via actions
- **Shared Knowledge Structures**: Blackboards, knowledge graphs, databases
- **Coordination Protocols**: discussed next
- **Discovery and Task Delegation**: Registry and indexing to locate appropriate agents or services

Student Questions

©2025 Raj Jain

Protocol Stacking

- Protocols define syntax, security, discovery, task delegation, and workflow orchestration across agents.
- Protocols allow abstracting away vendor differences and allow scalable echo systems
- Some protocols connect agents to external tools/data.
- Some enable agents to find and communicate with peers.
- Some orchestrate multi-agent workflows and manage state.
- Domain-specific protocol stacks, e.g., for healthcare and finance, are being developed

Student Questions

©2025 Raj Jain

Agent Communication Protocols

1. Knowledge Query and Manipulation Language (KQML)
2. Foundation for Intelligent Physical Agents (FIPA) Agent Communication Language (ACL)
3. Model Context Protocol (MCP)
4. Agent-to-Agent (A2A)
5. Agent Coordination Protocol (ACP)
6. Agent Network Protocol (ANP)

Student Questions

Ref: A. Ehtesham, et al, "A survey of Agent Interoperability Protocols: Model Context Protocol (MCP), Agent Communication Protocol (ACP), Agent-to-Agent Protocol (A@A) and Agent Network Protocol (ANP)," 23 May 2025, 20 pp., https://arxiv.org/pdf/2505.02279v1

©2025 Raj Jain

Knowledge Query and Manipulation Language (KQML)

- Developed in the early 1990s as a part of the DARPA knowledge sharing effort.
- Provides a language and a protocol for agents to exchange information and knowledge.
- Designed for knowledge-based and distributed AI systems
- Defined a rich set of **performatives**, e.g., ask-one, tell, register, forward, for querying, asserting, and manipulating knowledge
- Messages have three layers: a communication layer (sender, receiver), a message layer (performative, language, ontology), and a content layer
- Primarily used in academic/research systems

Student Questions

©2025 Raj Jain

FIPA Agent Communication Language (FIPA-ACL)

- Developed from 1995 to 2000 by the "**Foundation for Intelligent Physical Agents (FIPA)** – a standardization consortium to create a formal standardized specification
- Standardized the KQML informal definitions and addressed ambiguities for interoperability
- Uses a rigorous semantic framework based on modal logic described in terms of an agent's beliefs, desires, and intentions
- Preferred for enterprise-grade commercial systems
- FIPA-ACL is one of a broader set of FIPA standards that define the entire Agent Management System

Student Questions

©2025 Raj Jain

Tools vs. Agents

- Agents can invoke tools and other agents
- Tools are rather fast, generally stateless, and return the responses synchronously
- Agents require more time. They generally return information asynchronously as it becomes available.
- Agents can have memory.
- MCP defines how to invoke tools. While other protocols, e.g., ACP, A2A, and ANP, define how to invoke agents.

Student Questions

©2025 Raj Jain

Model Context Protocol (MCP)

- Introduced by Anthropic in 2024.
- Many companies have adopted it because Anthropic delivered documentation and samples to enable the community to build MCP servers.
- The original goal was to add tools to the environment, like Claude.
- Standardizes LLM access to APIs and databases. Supports real-time permissioned integration. Used in toolchains.
- Client Application (Host) initiates the interactions with MCP server(s).

Student Questions

Ref: "What is the Model Context Protocol (MCP)? - Model Context Protocol,"
https://modelcontextprotocol.io/docs/getting-started/intro

©2025 Raj Jain

MCP Client

- Initializes sessions, requests, and processes for four core primitives: *Resources (Files, Audio, Video,…), Tools (Retrieve, Search, Update, …), Prompts (Pre-defined templates) and Sampling*.
- Also, handles asynchronous *notifications* related to server-side events.
- Implements robust *error-handling* routines and timeouts to ensure reliable coordination
- Each session goes through initialization, operation, and shutdown

Student Questions

©2025 Raj Jain

MCP Server

- Provides data, services, and interaction templates for clients
- Exposes and manages contextual *resources*
- Executes external operations via *Tools*
- Defines Reusable *prompts* for consistent interactions
- Delegates the text-generation task through *sampling*
- Enforces access control policies
- Emits *notifications* to reflect changes in its available capabilities

Student Questions

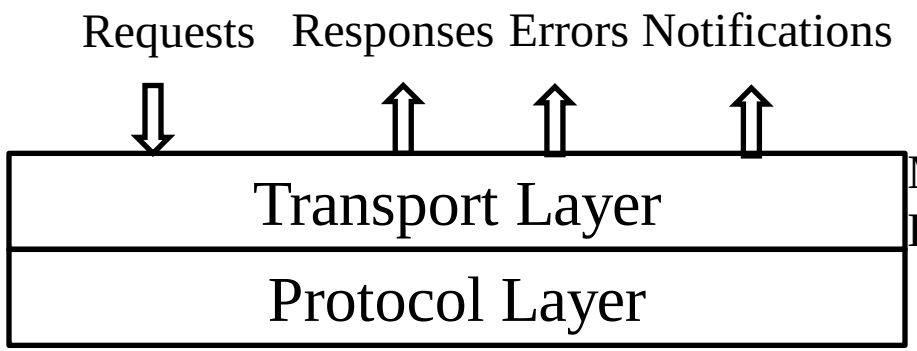
©2025 Raj Jain

MCP Components

Clients
Claude Desktop,
Script, …

Servers
Docusign, Github, Discord,
Shopify, …

Initiate Tools (Search, …) Request resources Build Prompts	Makes tools available Shares Resources Hosts Prompt Templates



Manages Client-Server comm:
Local or Remote

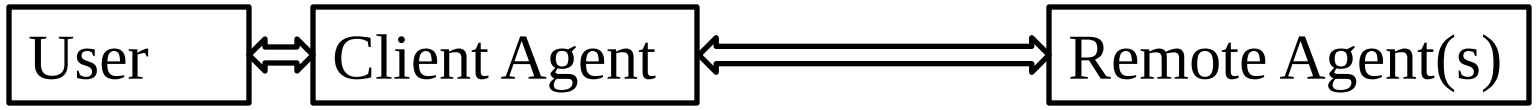
Matches Req./Resp.

Student Questions

©2025 Raj Jain

Agent-to-Agent Protocol (A2A)

- Open standard initiated by Google in the **Linux Foundation** for direct agent *messaging*, *agent cards*, and *capability advertising* for enterprise-scale task orchestration.
- User originates the interaction.
  The user could be a human or another agent
- User does not directly interact with the remote agent.
  It relies on the client agent to translate into actionable tasks.
- In multi-agent hierarchies, an agent can trigger downstream actions by another agent



Student Questions

©2025 Raj Jain

A2A Client Agent

- Represents the user's intent and coordinates with remote agents
- May span multiple stages of a task lifecycle
- Begins by performing Agent Discovery, retrieving and evaluating agent cards
- Agent cards describe the agent's capabilities, skills, input/output specifications, and authentication requirements
- Initiates a task by constructing a task object (e.g., contract) for the selected remote agent
- Oversees error Handling
- Presents the results to the user
- May also handle asynchronous notifications

Student Questions

©2025 Raj Jain

A2A Remote Agent

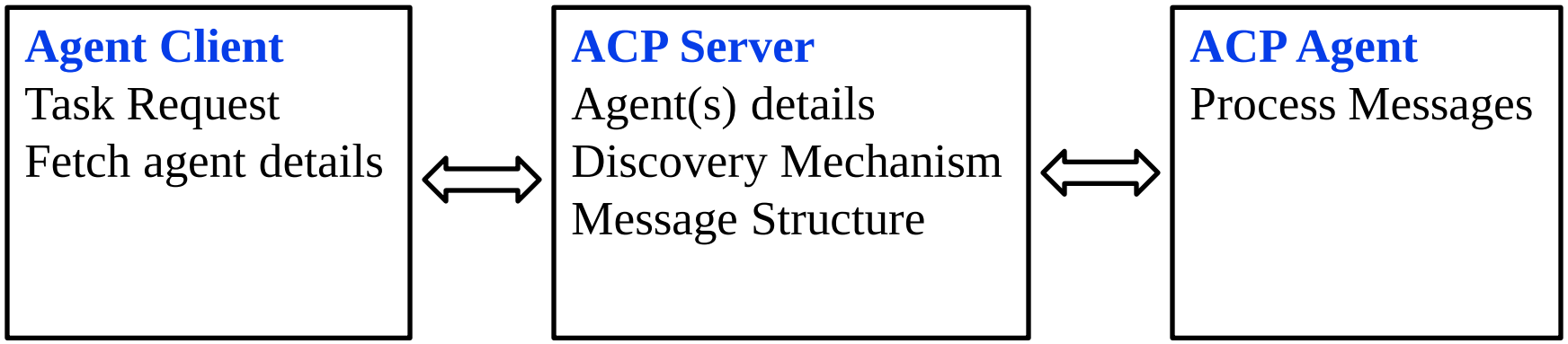
- Provides one or more skills (capabilities)
  e.g., an agent with discovery skill can discover other agents
- Each skill is formally defined by its input and output schema
- Publishes an Agent Card – a structured metadata document that includes kills, usage instructions, and authentication instructions
- Executes the tasks delegated by the client agent.
- Manages its internal resource usage, ensuring fair allocation of compute, memory, network, and storage resources
- Enforces security and authentication requirements

Student Questions

©2025 Raj Jain

Agent Communication Protocol (ACP)

- Introduced by IBM.
- Standardizes discovery, invocation, and interaction among AI agents
- Agent Client discovers other agents through a published registry
- ACP Server acts as a protocol broker. It maintains Agent Registry, a metadata catalog, and enforces system-wide policies, including authentication



Student Questions

©2025 Raj Jain

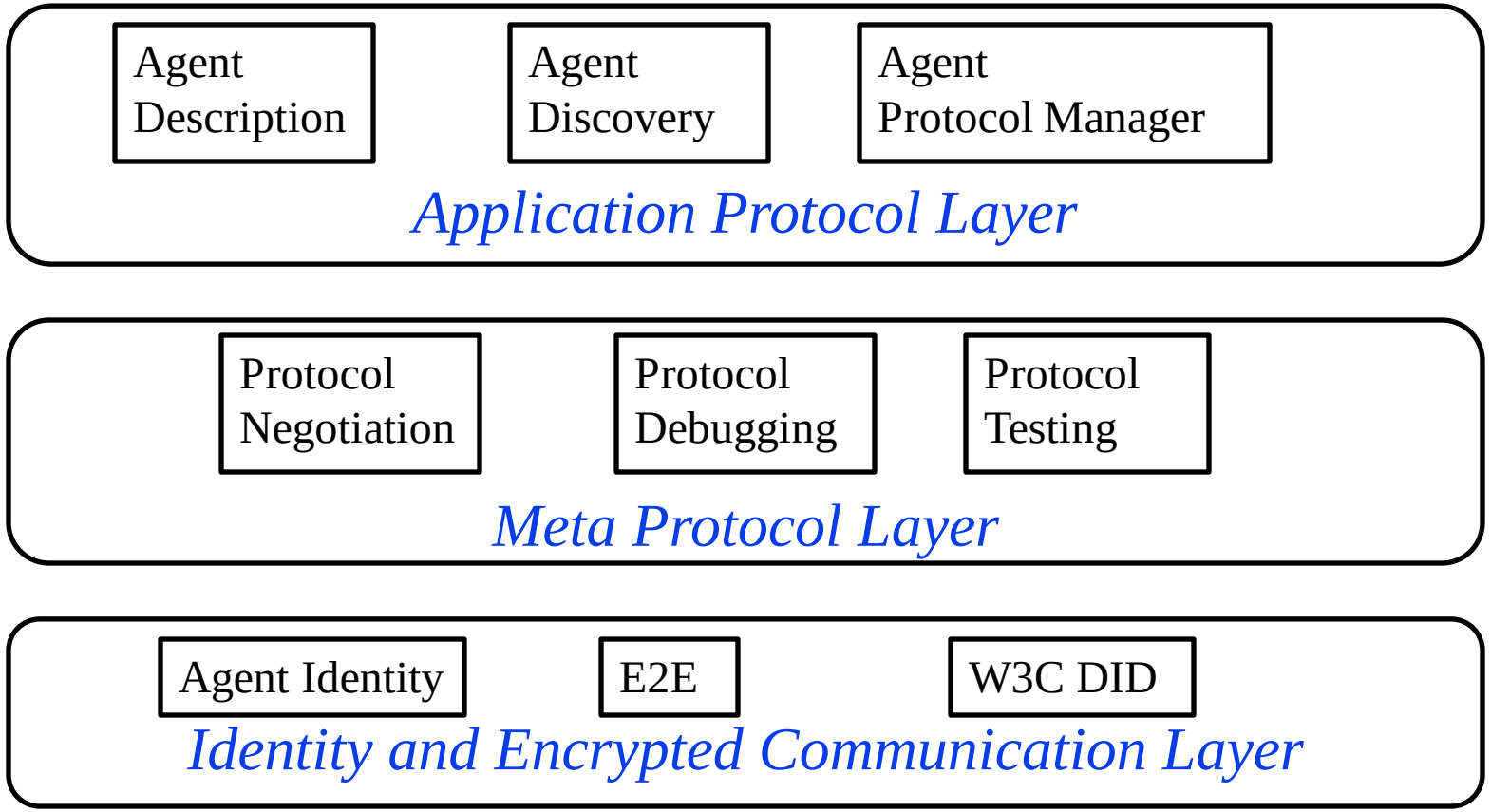
Agent Network Protocol (ANP)

- *Decentralized*, Peer-to-peer, identity-forward model for cross-platform agent interactions on the open internet
- ANP enables agents to autonomously discover, authenticate, and interact using structured metadata
- A decentralized discovery and collaboration protocol built on *decentralized identifiers* (DIDs) and JSON-LD graphs for Open-Internet agent marketplaces
- Uses World-Wide-Web Consortium (W3C)'s DIDs

Student Questions

©2025 Raj Jain

ANP Overview



Student Questions

©2025 Raj Jain

Networking Challenges in IoAA

1. **Latency**: Many applications require millisecond-scale responses, e.g., intersection safety
2. **Scalability**: Orchestrating thousands and millions of agents requires robust discovery, routing, and identity management
3. **Bandwidth/Overhead**: Too much messaging and large exchanges stress the network
4. **Fragility and Reliability**: With an increasing number of agents, the risk of cascading failures, bottlenecks, and data inconsistency increases.
5. **Security/Trust**: Threats of impersonation, eavesdropping, prompt injection, or unauthorized executions
6. **Interoperability**: Inter-vendor interoperability requires strong standards

Student Questions

©2025 Raj Jain

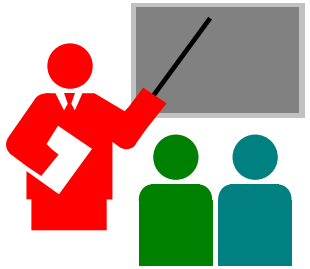
Comparison of IoAA Protocols

Aspect	MCP	ACP	A2A	ANP
Architecture	Client-Server	Brokered Client-Server	Peer. Client – Remote Agent	Decentralized Peer-to-Peer
Agent Discovery	Manual registration	Registry-based	Agent cards	Search engine discovery
Core Components	Tools, Prompts, Resources, Sampling	Agent Detail, Message, Task Request, Artifact	Agent Card, Task, Message, Artifact	Agent description, Structured Interface
Transport	HTTP, stdio, server-sent events (SSE)	HTTP	HTTP with optional SSE, Push notifications	HTTP over TLS
Session support	Stateless + optional persistent tool context	Stateful	Stateful or stateless	Stateless
Target Scope	LLM-External Tool/Service	Model-agnostic Infrastructure-level agents	Trusted enterprise task delegation	Open Internet Agent interconnectivity
Strengths	Tight LLM integration	Multimodal messaging, brokered registry, tool modularity	Inter-agent negotiation, artifact-driven, delegation	DID-based trustless identity
Limitations	Centralized server	Registry required	Enterprise-centric	Negotiation overhead

Student Questions

©2025 Raj Jain

Summary



1. AI agents do AI tasks for users.
2. Agents can be generic (for all applications) or specific, such as healthcare, video, legal, etc.
3. Examples of generic AI agents are Copilot, Gemini, Claude, …
4. Autonomous Agents are called Agentic AI.
5. Agents make use of other agents to complete a task
6. Several protocols for Internet of AI agents were discussed:
7. MCP uses URL lookup to find other agents. ACP uses a registry of Agents. A2A servers collect agent cards. ANP uses decentralized agents.

Student Questions

Required Reading

- A. Ehtesham, et al., "A Survey of Agent Interoperability Protocols: Model Context Protocol (MCP), Agent Communication Protocol (ACP), Agent-to-Agent Protocol (A2A), and Agent Network Protocol (ANP)," May 4, 2025, https://arxiv.org/html/2505.02279v1

Student Questions

References

- G. Rathor, "Understanding MCP, ACP, and A2A," IBM Data Community Blog, June 26, 2025, https://community.ibm.com/community/user/blogs/gyanendra-s-rathor/2025/06/26/understanding-mcp-acp-and-a2a
- N. Heidloff, "Comparison of Agent Protocols MCP, ACP and A2A," Blog, Sep 16, 25, https://heidloff.net/article/mcp-acp-a2a-agent-protocols/
- Meenal, "Agentic AI Protocols: MCP vs A2A vs ACP vs ANP,"July 24, 2025, https://k21academy.com/ai-ml/agentic-ai/agentic-ai-protocols-comparison/
- M. Zodge, "The Agent Protocol Wars: A Complete Guide to MCP, A2A, ANP, and ACP," LinkedIn, June 26, 2025, https://www.linkedin.com/pulse/agent-protocol-wars-complete-guide-mcp-a2a-anp-acp-milind-zodge-2tkxc/
- J. Rosenberg, C. Jennings, "Framework, Use Cases and Requirements for AI Agent Protocols," IETF draft, May 5, 2025, https://www.ietf.org/archive/id/draft-rosenberg-ai-protocols-00.html

Student Questions

©2025 Raj Jain

Acronyms

- ACL ACL is one of a broader set of FIP
- ACP Agent Coordination Protocol
- AI Artificial Intelligence
- ANP Agent Network Protocol
- API Application Programming Interface
- DARPA Defense Advanced Research Projects Agency
- DID Decentralized Identifiers
- FIPA Foundation forl Intelligent Physical Agents
- IBM International Business Machines
- IETF Internet Engineering Taks Force
- IoAA Internet of AI Agents
- JSON Java Script Object Notation
- KQML Knowledge Query and Manipulation Language

Student Questions

Acronyms (Cont)

- LD Linked Data
- LLM Large Language Models
- MAS Multi-Agent Systems
- MCP Model Context Protocol
- RAG Retrieval-Augmented Generation
- URL Universal Resource Locator

Student Questions

©2025 Raj Jain

Scan This to Download These Slides



Raj Jain
http://rajjain.com

http://www.cse.wustl.edu/~jain/cse5700-25/m_14ioa.htm

Student Questions

©2025 Raj Jain

Related Modules



CSE 567: The Art of Computer Systems Performance Analysis
https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n_1X0bWWNyZcof

CSE473S: Introduction to Computer Networks (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcgy5e_10TiDw





CSE 570: Recent Advances in Networking (Spring 2013)
https://www.youtube.com/playlist?list=PLjGG94etKypLHyBN8mOgwJLHD2FFIMGq5

CSE571S: Network Security (Spring 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypKvzfVtutHcPFJXumyyg93u





Video Podcasts of Prof. Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw

Student Questions