Beyond Self-Talk: A Communication-Centric Survey of LLM-Based Multi-Agent Systems

Bingyu YAN¹, Zhibo ZHOU², Litian ZHANG⁴, Lian ZHANG¹, Ziyi ZHOU¹, Dezhuang MIAO¹, Zhoujun LI³, Chaozhuo LI⁴, Xiaoming ZHANG¹⊠

- 1. School of Cyber Science and Technology, Beihang University, Beijing 100191, China
- 2. The College of Cyber Security/College of Information Science and Technology, Jinan University, Guangzhou, China
- 3. School of Computer Science and Engineering, Beihang University, Beijing 100083, China
- 4. School of Cyber Science and Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

E-mail: yolixs@buaa.edu.cn.

Abstract

Large language model-based multi-agent systems have recently gained significant attention due to their potential for complex, collaborative, and intelligent problem-solving capabilities. Existing surveys typically categorize LLM-based multi-agent systems (LLM-MAS) according to their application domains or architectures, overlooking the central role of communication in coordinating agent behaviors and interactions. To address this gap, this paper presents a comprehensive survey of LLM-MAS from a communication-centric perspective. Specifically, we propose a structured framework that integrates system-level communication (architecture, goals, and protocols) with system internal communication (strategies, paradigms, objects, and content), enabling a detailed exploration of how agents interact, negotiate, and achieve collective intelligence. Through an extensive analysis of recent literature, we identify key components in multiple dimensions and summarize their strengths and limitations. In addition, we highlight current challenges, including communication efficiency, security vulnerabilities, inadequate benchmarking, and scalability issues, and outline promising future research directions. This review aims to help researchers and practitioners gain a clear understanding of the communication mechanisms in LLM-MAS, thereby facilitating the design and deployment of robust, scalable, and secure multi-agent systems.

Key words

large language model; LLM-based multi-agent systems; communication-centric framework; agent communication protocols

■ 1 Introduction

Large language models (LLMs) have recently demonstrated significant potential across diverse domains. Building upon these strengths, LLMs have been integrated into autonomous agents equipped with profiling, memorization, planning, and action modules [1]. To make agents more coordinated and scalable when handling complex or dynamic tasks [2], LLM-based multi-agent systems (LLM-MAS) have been proposed, where multiple agents interact to achieve goals that exceed the capacity of a single agent. Recent studies underscore LLM-MAS effectiveness in contexts ranging from social simulation [3], to software engineering [4], and recommendation systems [5], illustrating the growing demand for more coordinated and intelligent multi-agent systems (MAS).

Given the broad application scope and research potential of LLM-MAS, several surveys have appeared to provide researchers with a systematic overview of this emerging research area. These surveys can be broadly categorized into two types: general surveys and domain-specific surveys. As shown in Fig. 1 (a), general surveys typically focus on system architectures, agent-level actions, and potential application

scenarios [6–8]. However, they often provide limited coverage of the communication and coordination workflows among agents, which are critical for effective multi-agent collaboration. As shown in Fig. 1 (b), domain-specific surveys delve into particular use cases such as social simulation [9] or software engineering [10, 11]. While offering indepth analyses of domain-specific LLM-MAS workflows, these studies lack generalizability and fail to propose a comprehensive framework for broader applications.

Inter-agent communication plays a critical role in enabling LLM-MAS to perform more complex tasks compared to single-agent systems by facilitating idea exchange and coordinated planning. Drawing on insights from traditional communication theory [12,13], concepts such as "source" and "channel" align closely with the communication processes present in the LLM-MAS workflow. Consequently, as shown in Fig. 1 (c), the LLM-MAS workflow can be effectively decomposed through a communication-centric perspective. Specifically, we define LLM-MAS as a communication protocol-constrained automated system driven by communication goals within a predefined communi-

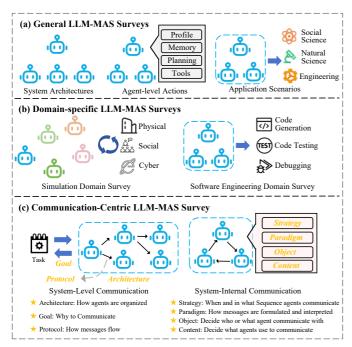


Fig. 1 Position of this survey within existing LLM-MAS literature. The figure contrasts prior general and domain-specific surveys with the communication-centric perspective, underscoring the need for a cross-cutting framework that spans tasks, architectures, workflows, and interaction between agents

cation architecture. Agents in this system have multiple communication strategies and paradigms, interacting with various communication objects to exchange diverse content for task completion.

Fig. 2 summarizes the structure of this survey. To provide necessary context, Section 2 introduces foundational concepts and terminology relevant to LLM-MAS. Building upon this, we propose a two-level analytical framework distinguishing between system-level communication and system-internal communication, discussed respectively in Section 3 and Section 4. The system-level communication analysis addresses how agents are organized, their overarching communication goals, and key emerging protocols. In contrast, the system-internal communication dynamics among agents, examining their strategies, paradigms, communication objects, and exchanged content. Subsequently, Section 5 highlights current challenges and outlines promising research opportunities. This structure provides a holistic understanding of the workflow across varied tasks.

Our main contributions include:

- Comprehensive Framework: From a communication perspective, we designed a comprehensive framework applicable to all types of LLM-MAS, analyzing the workflow at both the system level and the internal system level.
- Deep Analysis of Communication Processes: We dissect realworld examples and prototypes to illustrate how well-orchestrated communication leads to more effective multi-agent behavior.
- Identification of Challenges and Opportunities: We shed light on open issues like scalability, security, and multimodal in-

tegration, and offer potential research directions for both academia and industry.

■ 2 Background

This chapter provides the conceptual grounding for the remainder of the survey. We first revisit the internal structure and operating principles of LLM-based single agents. Then introducing the traditional multi-agent systems (MAS). We conclude by articulating how LLM-MAS inherit, extend, and occasionally challenge the assumptions of earlier paradigms, thereby motivating the communication-centric taxonomy developed in subsequent sections.

2.1 LLM-Based Agents

LLM-based agents are autonomous entities whose core reasoning component is a LLM. They represent the cornerstone of multi-agent architectures, as they lay the groundwork for understanding how individual agents reason, plan, and act. In line with the taxonomy proposed by [14], this section outlines the composition and functionalities of LLM-based agents.

An LLM-based agent typically consists of three key components: *Brain*, *Perception*, and *Action*, each playing a distinct yet complementary role. 1) **Brain** is a LLM that integrates both short-term and long-term memory modules to reduce potential hallucinations and enhance the agent's reasoning and planning capabilities. Short-term memory caches the current conversational context while long-term memory stores structured artefacts accumulated across sessions. Various retrieval augmented generation (RAG) methods [15] and RAG enhancement research [16] play an important role in enhancing memory modules. 2) **Perception** is a multimodal interface that converts raw sensory inputs including text, vision, audio, or environmental state vectors into prompts consumable by the Brain. 3) **Actions** are not limited to generating textual responses, they also encompass integration with external tools such as web APIs or real-world actuators [17, 18] to enhance the agent's problem-solving capabilities.

2.2 Traditional Multi-Agent Systems

Before the rise of LLMs, the MAS research had established a rich toolbox spanning symbolic reasoning and learning-based coordination [19]. Early symbolic MAS describe agents in terms of Beliefs, Desires, and Intentions and prescribe communication via agent-communication languages. These languages provide machine-interpretable speech acts such as inform, request and propose, and support standard protocol templates including contract nets and auction-based negotiation, thereby ensuring transparent reasoning about commitments, goals, and obligations. However, their discrete vocabularies and brittle parsers make them ill-suited for open-domain tasks.

The learning-based MAS replaces handcrafted rules with optimisation. Centralised-training-with-decentralised-execution frameworks [20] use a global critic to stabilise gradients while permitting fully distributed policies at test time. Independent Q-learning and policy-gradient variants alleviate non-stationarity, whereas value-decomposition, counterfactual baselines, and influence-based credit

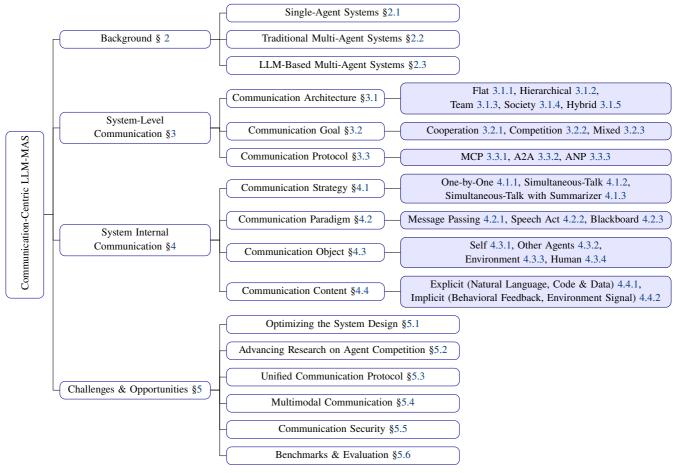


Fig. 2 The structure of this paper

assignment attack the credit-assignment problem directly. Graph neural agents, in turn, convey compact latent messages over dynamic communication graphs and scale to hundreds of cooperative robots, traffic-signal controllers, or swarm drones. Nonetheless, most learning-based systems still adopt narrow, task-specific message formats, incur heavy sample complexity, and provide limited interpretability which motivated the search for language-native coordination.

2.3 LLM-Based Multi-Agent Systems

While single-agent systems exhibit strong individual reasoning, they often struggle with tasks requiring collective intelligence or large-scale coordination. MAS [21] can address these limits by orchestrating multiple intelligent agents and leveraging communication as a key mechanism for goal alignment. Meanwhile, LLM-MAS combine the linguistic flexibility of LLM agents with the coordination principles of MAS, thereby dissolving the boundary between natural-language dialogue and agent communication. Agents can cooperate, compete, or negotiate, depending on system objectives and architectural choices. Such flexibility in communication design sets the stage for LLM-MAS, where advanced language models enable more sophisticated inter-agent interactions across diverse application domains.

■ 3 System-Level Communication

In this section, the LLM-MAS is analyzed from the macro systemlevel communication. We first examine the communication architecture, highlighting how different architectures such as flat, hierarchical or society-based organize agents. Each of these architectures offers distinct approaches to agent interaction, with implications for scalability, flexibility, and efficiency in system performance. We then delve into the communication goals that decide why agents communicate, where cooperation, competition, or a mixture of both can lead to distinct multi-agent dynamics. Through specific application examples, we demonstrate the advantages, limitations, and applicable scenarios of these communication architectures and goals. Finally, this section discusses the emerging communication protocols and introduces three prominent protocols in detail to clarify the standardized communication behavior. As shown in Table 1, because the communication protocol has not been widely studied and used, we categorize current LLM-MAS studies according to the communication architectures and communication goals in detail.

3.1 Communication Architecture

Communication architecture defines the structural organization of agents within a LLM-based multi-agent system and governs the flow of infor-

Table 1 Representative LLM-MAS studies grouped by communication architecture and communication goal

| Architecture | Goal | Work | | |
|--------------|-------------------------------------|---|--|--|
| Flat | Cooperation Competition Mixed | | | |
| Hierarchical | Cooperation | ChatDev [29]; AutoDefense [30]; CausalGPT [31]; SoA [32]; FINCON [33]; Wang et al. [34]; CoA [35]; AutoData [36]; AutoHMA-LLM [37]; G-Safeguard [38]; Li et al. [39]; Kalyuzhnaya et al. [40]; LogiAgent [41]; MACM [42]; CPDESIM [43]; Shen et al. [44]; EvoMAC [45]; Wang et al. [46] | | |
| | Competition Mixed | Cai et al. [3] Ju et al. [47]; Wu et al. [48] | | |
| Team | Cooperation Mixed | MetaGPT [4]; MAGIS [49]; AgentCoord [50]; AutoAgents [51]; Qian et al. [52]; SimClass [53]; Fan et al. [54]; Ma et al. [55]; FactGuard [56]; Luo et al. [57]; MDTeamGPT [58]; MedAgents [59]; Thematic-LM [60] POLCA [61]; ReCon [62] | | |
| Society | Cooperation Mixed | Generative Agents [63]; GOVSIM [64]; Yue et al. [65]; Sreedhar et al. [66] Dai et al. [67]; EconAgent [68]; Guan et al. [69]; EcoLANG [70] | | |
| Hybrid | Cooperation | FixAgent [71]; PeerGPT [72]; ChatSim [73]; Tulip Agent [74]; MADR [75]; AgentFM [76]; Ronanki et al. [77]; Zhang et al. [78]; Flow-of-Action [79]; Wang et al. [80] Agent4Debate [81]; Zhang et al. [82] | | |
| | Competition Mixed | Wu et al. [83]; BlockAgents [84]; Xu et al. [85]; ToM [86]; TED [87] | | |

mation among them [88]. It significantly influences both macro-level system behaviors and micro-level interactions, shaping aspects like scalability, flexibility, and operational efficiency. The choice of architecture usually depends on task complexity, agent autonomy levels, and desired interaction patterns. As shown in Fig. 3, we explore five primary communication architectures: Flat, Hierarchical, Team, Society, and Hybrid architectures, providing additional detailed discussions and examples to deepen understanding.

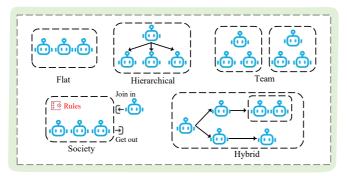


Fig. 3 Five canonical communication architectures for LLM-MAS

3.1.1 Flat Architecture

Flat architecture is characterized by a decentralized network of peerto-peer agent interactions without hierarchical distinctions or central oversight. This architecture excels in environments requiring agile, flexible, and spontaneous interactions among agents, such as dynamic task assignments and rapid decision-making scenarios. For example, Abdullin et al. [23] demonstrate flat architecture effectiveness in generating synthetic dialogues, where agents collaboratively and iteratively refine outputs. Similarly, Du et al. [24] employ a flat architecture for fact-checking, enabling agents to critique each other's reasoning dynamically, thereby enhancing overall accuracy and reducing hallucinations. Despite its benefits in adaptability and responsiveness, a flat structure can encounter challenges in scalability, as increased agent count may lead to increased communication overhead and reduced coordination efficiency.

3.1.2 Hierarchical Architecture

In hierarchical architectures, agents are structured into layers or tiers, with higher-level agents responsible for strategic oversight and lower-level agents performing detailed execution tasks. This configuration is particularly effective for complex scenarios demanding clear task delegation, supervision, and integration of diverse agent competencies. For instance, ChatDev [29] organizes agents into specialized roles such as designers, coders, and testers under senior management agents, effectively facilitating software development through structured workflows. CausalGPT [31] exemplifies hierarchical use by employing higher-level evaluators to guide lower-level agent reasoning, thereby significantly improving output consistency. However, hierarchical systems may encounter bottlenecks, particularly when higher-level agents become overloaded or communication delays between layers emerge.

3.1.3 Team Architecture.

Team-based architectures segment agents into specialized groups or teams, each focusing on distinct tasks or domains, thus leveraging specific agent expertise and fostering robust intra-team collaboration. For instance, MAGIS [49] demonstrates the benefits of team architecture by categorizing agents into administrators, developers, and testers, streamlining the collaborative resolution of software issues on platforms such as GitHub. The POLCA framework [61] further illustrates team architecture versatility by employing specialized teams to simulate political negotiations, predicting coalition formation outcomes. While team architectures effectively leverage specialized expertise, the increased inter-team communication demands can introduce additional overhead, necessitating efficient cross-team coordination mechanisms.

3.1.4 Society Architecture

Society architectures model agent interactions within broader social environments governed by shared norms or rules, reflecting emergent behaviors characteristic of human societies. These architectures support complex, large-scale simulations involving diverse agents with varying roles, motivations, and interactions. Generative Agents [63], for example, create sandbox environments where agents dynamically form friendships, organize activities, and adapt behaviors based on past experiences. EconAgent [68] integrates economic dynamics into agent behaviors, simulating realistic economic decisions like consumption, investment, and employment, thus providing insights into macroeconomic phenomena driven by micro-level actions. Although society architectures excel at simulating emergent phenomena and social interactions, they can become challenging to manage due to the inherent complexity and unpredictability of agent behaviors.

3.1.5 Hybrid Architecture

Not all designs fit neatly into a particular architecture, and some architectures may contain features from several different styles. Hybrid architectures combine multiple communication structures to create flexible and adaptable multi-agent systems capable of addressing diverse challenges. By integrating hierarchical oversight with decentralized agent collaboration, hybrid architectures optimize agent interactions and resource allocation dynamically. FixAgent [71] exemplifies hybrid architectures by adapting hierarchical structures to debugging tasks, combining strategic oversight with decentralized task execution. ChatSim [73] integrates top-down control for scene rendering with peer-to-peer collaboration among agents for detailed asset integration, thus overcoming limitations inherent to purely hierarchical or flat systems. Tulip Agent [74] employs a hybrid approach enabling agents to dynamically discover and utilize tools, showcasing enhanced flexibility, adaptability, and scalability across multiple scenarios. However, hybrid systems require sophisticated design strategies to avoid coordination overhead and ensure efficient operation.

In summary, the choice of communication architecture significantly influences the capabilities, efficiency, and scalability of LLM-based multi-agent systems. Researchers and practitioners must carefully evaluate their specific requirements, considering trade-offs between flexibility, control, scalability, and efficiency, to select the most suitable architecture or combination thereof.

3.2 Communication Goal

Communication goals represent the intended purpose behind agent interactions, driving behaviors, information-sharing patterns, and coordination strategies within a multi-agent system. Clearly articulating these goals enhances system efficiency, coherence, and adaptability to diverse scenarios, as they encapsulate the "why" behind the communication. As shown in Fig. 4, this section elaborates on three primary communication goals: Cooperation (including Direct Cooperation and Cooperation through Debate), Competition, and Mixed goals.

3.2.1 Cooperation

Cooperation is a central feature in numerous multi-agent scenarios, which involves agents collaboratively working towards shared objectives, leveraging collective knowledge and skills to achieve outcomes superior to those achievable individually. Within cooperative settings, interactions are often characterized by transparency, mutual trust, and

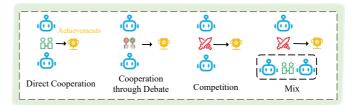


Fig. 4 Communication goals driving multi-agent interaction

a focus on common goals. Cooperation is divided into two main types: direct cooperation and cooperation through debate.

Direct cooperation refers to straightforward and seamless collaboration where agents openly share information and resources to jointly complete tasks or solve problems. This interaction style emphasizes rapid consensus and efficient integration of expertise, critical in time-sensitive or complex problem-solving environments. For instance, some works harness direct cooperation to enhance LLM reasoning [22, 31, 51], while others employ it in collaborative code generation [29, 32, 49, 52, 71] and scientific experimentation [73, 74]. The research community continues to explore advanced coordination models [34, 50, 64] for fine-grained task allocation, robust communication protocols, and scalability in agent collectives.

Cooperation through debate introduces a nuanced cooperative model where agents actively critique and refine each other's inputs through structured debates. Rather than passively accepting shared information, agents rigorously challenge each other's assumptions, reasoning, and outcomes to achieve more robust and accurate conclusions. Examples include factual reasoning [24] and fact-checking [75], where rigorous back-and-forth discussions help validate information and reduce the likelihood of mistakes. This method effectively balances collaborative interaction with critical evaluation, producing more resilient and well-rounded outcomes.

3.2.2 Competition

Competitive interactions in LLM-based multi-agent systems occur when agents have conflicting objectives or vie for limited resources or favorable outcomes. This adversarial context stimulates strategic thinking, innovation, and adaptive behaviors, as agents must continually refine their strategies to succeed.

The game-playing ability of agents in the system has been demonstrated in research GAMA–Bench [26]. In these adversarial contexts, agents actively shape the interaction by generating persuasive or deceptive narratives. For instance, the study by Cai et al. [3] explores language evolution within adversarial simulations, providing insights into how competitive interactions drive linguistic adaptation. Agent4Debate [81] designed a dynamic multi-agent framework for competitive debate with humans. One significant advantage of competition in LLM-MAS is its potential to drive innovation and strategic sophistication. As agents continually adjust to rivals' tactics and environmental feedback, they refine their own approaches in a never-ending loop of adaptation. For instance, [82] explored a poetry-generation task where agents strove to outperform each other through creative linguistic outputs.

However, competitive settings introduce a range of challenges, including potential instability and security vulnerabilities induced by adversarial or deceptive agent behaviors. Therefore, it is imperative to design mechanisms that carefully reconcile competitive incentives with cooperative regulatory constraints to ensure sustainable and robust system performance.

3.2.3 Mixed

While purely cooperative or purely competitive settings offer conceptual clarity, mixed communication goals blend cooperative and competitive elements, reflecting the complexity and fluidity of real-world interactions. Within these mixed regimes, agents continuously reconstitute alliances, vie for scarce resources, and initiate strategic collaborations as situational contingencies and task objectives evolve. Such flexibility enhances the system's capacity to tackle multi-faceted problems and to maintain robust performance under dynamically changing environmental conditions.

In practice, such mixed interactions are pivotal for capturing nuanced, dynamic behavior in domains like social simulations [47, 67], collective problem-solving, or negotiation tasks [61, 69]. Allowing agents to strike a balance between cooperative and adversarial behavior makes it possible to emerge solutions that cannot be suggested by purely cooperative or competitive environments.

Despite their versatility, mixed-goal interactions introduce complexities regarding mechanism design, protocol standardization, and ethical considerations. Balancing cooperation and competition dynamically necessitates sophisticated coordination and monitoring mechanisms to ensure system stability and ethical integrity.

In summary, clearly defining and structuring communication goals is critical to optimizing multi-agent interactions. Selecting and implementing appropriate goals depend heavily on task requirements, system scalability, and desired agent dynamics, ultimately influencing overall system effectiveness.

3.3 Communication Protocol

While the communication architecture decides who can talk to whom and the communication goal clarifies why they talk, a dedicated communication protocol specifies how the messages actually flow between agents and external systems. Standardized protocols are now emerging that make LLM-MAS deployments portable, secure, and easier to audit. Communication protocols detail the actual mechanics of interaction, ensuring consistent, secure, and efficient communication. As shown in Fig. 5. This section introduces three key emerging protocols: Model Context Protocol (MCP) [89], Agent-to-Agent Protocol (A2A) [90], and Agent Network Protocol (ANP) [91].

3.3.1 Model Context Protocol

MCP is a general-purpose context-oriented protocol developed to facilitate secure and structured interactions between LLM agents and external resources such as tools, data, and services. MCP utilizes a JSON-RPC client-server architecture, enabling agents (hosts) to request and receive context from external resources through intermediate components—clients and servers. In this architecture, the host initiates context requests based on user queries, and the client manages connections to both the host and server, providing resource descriptions and

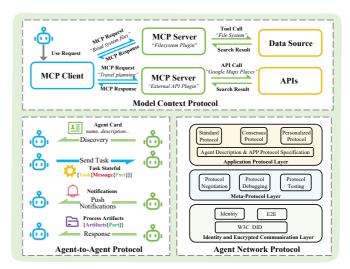


Fig. 5 Emerging communication protocols for LLM-MAS

executing context requests. The server directly interacts with resources to execute client requests and relay context, while resources include data, tools, or services. This layered approach reduces fragmentation across various agents and tool providers, significantly improving interoperability and scalability. Additionally, MCP enhances data security by decoupling sensitive tool invocations from LLM-generated responses, thus minimizing the risks of data exposure.

3.3.2 Agent-to-Agent Protocol

A2A supports inter-agent communication, emphasizing secure and structured peer-to-peer interactions among LLM agents. A2A employs capability-based "Agent Cards" distributed via HTTP and Server-Sent Events, facilitating efficient task outsourcing and collaboration within enterprise-scale deployments. Agents advertise their capabilities through Agent Cards, enabling dynamic task delegation based on real-time capability awareness. Communication occurs directly between peers without centralized intermediaries, significantly reducing latency and improving responsiveness. Additionally, asynchronous messaging via server-sent events enhances scalability and robustness. A2A's structured, capability-driven interactions improve task efficiency and collaboration fidelity, particularly suited for complex enterprise environments.

3.3.3 Agent Network Protocol

ANP facilitates decentralized agent communication and discovery over open networks. Built upon decentralized identifiers (DIDs) and JSON-LD graphs, ANP promotes secure, interoperable interactions among heterogeneous agents. Agents dynamically discover and verify peers using DIDs, ensuring secure identification across network boundaries. Communication is structured via JSON-LD graphs, enabling semantic clarity and context-aware interactions. ANP also incorporates encryption and secure channels, safeguarding data integrity and confidentiality. Its decentralized infrastructure supports robust, crossorganizational collaboration, fostering scalable and secure multi-agent ecosystems on a global scale.

Table 2 adapts the comparative framework proposed by Abul et

al. [92], complements it and extends it with additional dimensions such as security and use cases to better contextualise LLM-MAS. MCP, A2A, and ANP represent significant advancements in standardizing and enhancing communication within LLM-based multi-agent systems. Additionally, other emerging protocols such as Agent Communication Protocol (ACP) [93], Agent Interaction and Task Protocol (AITP) [94], and Agent Content Protocol (AConP) [95] are also gaining attention, highlighting the dynamic and evolving landscape of communication protocols. Collectively, these protocols address interoperability, security, scalability, and context management, paving the way toward more integrated and intelligent multi-agent deployments.

Table 2 Comparison of Three Emerging Agent Protocols

| Aspect | MCP | A2A | ANP |
|-------------|--|---|---|
| Topology | JSON/RPC over client–server channel | Peer-style client ↔ remote agent link | Decentralised P2P agent mesh |
| Discovery | Static endpoint or manual registry entry | Signed Agent Card retrieval via HTTP | Search-index crawling + DID document exchange |
| Format | Typed JSON-RPC 2.0 messages | Task & Artifact bundles | JSON-LD; meta-protocol negotiation |
| Security | Bearer tokens; optional DID claims; RBAC | OAuth 2 / enterprise IAM; mutual TLS | DID-based handshake; end-to-end encryption |
| Strengths | Seamless LLM tool calling; minimal bootstrap | Rich task delegation; vendor-backed ecosystem | Trustless identity; no single point of control |
| Limitations | Centralised service dependency; safety risks | Cross-team workflows; delegated multi-step automation | P2P logistics coordination; DAO-driven negotiation |
| Use Cases | Plugin APIs; retrieval-augmented O&A | Enterprise workflows; delegated multi-step tasks | P2P logistics; DAO/DeFi negotiation |

■ 4 System Internal Communication

Having established the overall system-level perspective, we now turn to the internal communication within the LLM-MAS. We first categorize and compare diverse communication strategies that determine when and in what sequence agents communicate. Next, we discuss the communication paradigms that frame the form and modality of these exchanges, followed by an examination of communication objects and content. These elements collectively define the richness, adaptability, and effectiveness of communication in LLM-MAS, ultimately shaping the system's capacity for coordination and problem-solving.

4.1 Communication Strategy

Communication strategies dictate how and when agents interact within an LLM-based multi-agent system. These strategies govern the timing, sequence, and structure of communication exchanges, significantly affecting system coherence, information accuracy, and the overall effectiveness of agent collaboration. As shown in Fig. 6, three widely adopted communication strategies are explored.

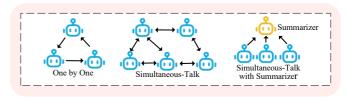


Fig. 6 The Communication Strategies of LLM-MAS

4.1.1 One-by-One

In the One-by-One communication strategy, agents communicate sequentially, each agent responding after fully processing and integrating all previous messages. This structured, turn-based approach maintains a clear context throughout interactions, significantly reducing misunderstandings and ensuring cohesive exchanges. The One-by-One strategy is particularly beneficial for tasks requiring methodical reasoning and detailed integration of inputs from multiple agents.

A typical example is Chain-of-Agents [35], which applies this strategy to manage lengthy text-generation tasks. Each agent summarizes previous contributions before providing its input, efficiently handling contexts beyond typical token limits.

Nevertheless, the strict serial dependency inherent in One-by-One communication imposes two key limitations as the agent population grows. First, latency scales linearly with the number of turns, because each agent must await the full completion of all preceding exchanges before contributing. Second, since inaccuracies introduced by early agents will unfold in each subsequent step, cumulative error propagation becomes more pronounced, posing a risk of semantic drift.

4.1.2 Simultaneous-Talk

The Simultaneous-Talk strategy allows agents to communicate concurrently, without waiting for turns. This strategy fosters a dynamic exchange environment conducive to rapid idea generation and parallel problem-solving. Simultaneous-Talk effectively leverages the diverse perspectives of multiple agents simultaneously, significantly enhancing brainstorming capabilities and uncovering creative solutions.

For instance, Autoagents [51] deploys multiple agents to generate ideas or solution paths concurrently. This parallel interaction model quickly reveals diverse possibilities, enhancing creativity and solution robustness. A similar pattern appears in EconAgent [68], where large-scale agents jointly conduct macroeconomic simulations.

Despite its advantages in agility and diversity, the Simultaneous-Talk approach introduces two key challenges. First, state staleness: without fine-grained synchronisation, agents may base their reasoning on outdated peer contributions, leading to logically inconsistent or redundant outputs. Second, conflict resolution: parallel proposals often overlap or contradict each other, necessitating an additional arbitration layer. Therefore, under this strategy, effective timestamps and lightweight consensus mechanisms are crucial.

4.1.3 Simultaneous-Talk-with-Summarizer

To address the challenges inherent in pure Simultaneous-Talk strategies, the Simultaneous-Talk with Summarizer strategy integrates a summarizing agent responsible for consolidating concurrent commu-

Table 3 Summary of current LLM-MAS studies with their Communication Strategy, Communication Paradigm, Communication Object, and Communication Content. For the strategy module, OO, ST, SS denote One-by-one, Simultaneous-Talk, Simultaneous-Talk-with-Summarizer; For the paradigm module, MP, SA, BB denote message passing, speech act, blackboard; For the object module, SE, OA, EN, HU denote self, other agents, environment, human; For the content module, EC, IC denote explicit and implicit content

| act, blackboard; For the object | | | | | |
|---------------------------------|----------|-------------|----------------|---------|---------|
| Work | Strategy | Paradigm | Object | Content | Time |
| Generative Agents [63] | ST, SS | MP | OA, EN | EC, IC | 04/2023 |
| Du et al. [24] | ST | MP, SA | OA | EC, IC | 05/2023 |
| ChatDev [29] | OO | MP, SA | OA | EC, IC | 07/2023 |
| MetaGPT [4] | SS | BB | OA, EN | EC | 08/2023 |
| CausalGPT [31] | OO, SS | MP, BB | OA, EN | EC | 08/2023 |
| AutoAgents [51] | ST | MP | OA | EC | 09/2023 |
| EconAgent [68] | ST | MP | OA, EN | EC, IC | 10/2023 |
| | ST | MP. SA | OA OA | EC, IC | 11/2023 |
| Chuang et al. [27] | | | | | |
| MedAgents [59] | OO, ST | MP | SE, OA, HU | EC, IC | 11/2023 |
| Wu et al. [48] | OO | MP | SE, OA, EN | EC, IC | 12/2023 |
| Qian et al. [52] | OO | MP, BB | OA | EC | 12/2023 |
| Ulmer et al. [22] | OO | MP | SE, OA | EC | 01/2024 |
| Abdullin et al. [23] | OO | MP | OA | EC | 01/2024 |
| Dai et al. [67] | ST | MP | OA | EC, IC | 01/2024 |
| Wang et al. [34] | OO | MP | OA | EC, IC | 02/2024 |
| POLCA [61] | SS | MP, SA | OA | EC | 02/2024 |
| | SS | | OA OA | EC | 02/2024 |
| ChatSim [73] | | MP, SA | | | |
| MADR [75] | SS | MP | OA | EC | 02/2024 |
| Wu et al. [83] | OO, ST | MP | OA | EC, IC | 02/2024 |
| GAMA-Bench [26] | ST | MP | OA | EC | 03/2024 |
| PeerGPT [72] | OO, SS | SA | OA, HU | EC | 03/2024 |
| AutoDefense [30] | OO, ST | MP | OA | EC | 03/2024 |
| AgentCoord [50] | SS | MP, SA | SE, OA, EN, HU | EC, IC | 04/2024 |
| MACM [42] | 00 | MP | SE, OA, EN | EC | 04/2024 |
| SoA [32] | 00 | MP | OA | EC | 04/2024 |
| | ST | | | | |
| Xu et al. [85] | | MP | OA | EC | 04/2024 |
| GOVSIM [64] | SS | MP | OA | EC | 04/2024 |
| FixAgent [71] | SS | MP | OA | EC | 04/2024 |
| MAGIS [49] | OO | MP | OA, EN | EC | 05/2024 |
| Cai et al. [3] | OO, SS | MP, SA | SE, OA, EN | EC, IC | 05/2024 |
| CoA [35] | OO | MP | OA | EC | 06/2024 |
| FINCON [33] | SS | MP | OA, EN | EC | 07/2024 |
| SimClass [53] | SS | MP | OA | EC | 07/2024 |
| BlockAgents [84] | SS | MP, SA | OA | EC, IC | 07/2024 |
| _ | SS | | | | |
| Tulip Agent [74] | | MP | OA | EC, IC | 07/2024 |
| Guan et al. [69] | ST | MP, SA | OA | EC, IC | 07/2024 |
| Ju et al. [47] | OO | MP | OA | EC, IC | 07/2024 |
| Agent4Debate [81] | SS | MP | OA, EN | EC | 08/2024 |
| ToM [86] | ST | MP | OA, EN | EC | 08/2024 |
| Zhang et al. [82] | ST | MP | OA | EC | 09/2024 |
| Li et al. [39] | SS | MP | OA, EN | EC | 09/2024 |
| Kalyuzhnaya et al. [40] | SS | MP | OA, EN, HU | EC | 10/2024 |
| EvoMAC [45] | SS | MP, SA | OA, EN | EC, IC | 10/2024 |
| | SS | | | | |
| ReCon [62] | | MP, SA | OA CA FIN | EC, IC | 11/2024 |
| Fan et al. [54] | ST | MP, SA | OA, EN | EC | 01/2025 |
| Wang et al. [80] | SS | MP | SE, OA, HU | EC | 01/2025 |
| Luo et al. [57] | SS | MP | SE, OA, EN | EC | 01/2025 |
| Ma et al. [55] | OO | MP, SA | OA | EC | 02/2025 |
| Sreedhar et al. [66] | OO | MP | OA, EN | EC | 02/2025 |
| G-Safeguard [38] | SS | MP | OA, EN | EC | 02/2025 |
| Wang et al. [46] | SS | MP | OA, EN | EC | 02/2025 |
| Flow-of-Action [79] | SS | MP, SA | OA, EN | EC, IC | 02/2025 |
| | | | | | |
| Yue et al. [65] | SS | MP | SE, OA, EN, HU | EC, IC | 02/2025 |
| CODESIM [43] | 00 | MP | SE, OA, EN | EC | 02/2025 |
| LogiAgent [41] | OO | MP, BB | SE, OA, EN | EC | 03/2025 |
| GameChat [28] | SS | SA | SE, OA | EC | 03/2025 |
| MDTeamGPT [58] | SS | MP | SE, OA, EN, HU | EC | 03/2025 |
| AgentFM [76] | OO, ST | MP, SA | OA, EN | EC | 04/2025 |
| AutoHMA-LLM [37] | OO | MP | OA, EN | EC | 04/2025 |
| FactGuard [56] | OO, ST | MP | OA, EN | EC | 04/2025 |
| | | | OA, EN | | 04/2025 |
| Thematic-LM [60] | OO, ST | MP MD CA | | EC | |
| AutoData [36] | OO, ST | MP, SA | OA, EN | EC | 05/2025 |
| EcoLang [70] | ST | MP, BB | OA, EN | EC, IC | 05/2025 |
| Ronanki et al. [77] | OO, ST | MP | OA, HU | EC | 05/2025 |
| Zhang et al. [78] | ST | MP, BB | OA, EN, HU | EC, IC | 05/2025 |
| _ | OO | MP | SE, OA | EC | 05/2025 |
| Group Think [25] | | | | | |
| Shen et al. [44] | SS | MP | SE, OA, EN, HU | EC, IC | 05/2025 |

nications into coherent summaries. This summarizer periodically synthesizes inputs from multiple agents into concise, unified messages, ensuring that all agents remain aligned with the overall system context.

The hierarchical and team-based coordination scenarios, exemplified by CausalGPT [31] and AgentCoord [50], utilize summarizers to aggregate communication outcomes, facilitating clear decision-making and task delegation.

Although introducing a summarizer agent effectively mitigates synchronization issues, it reintroduces some sequential dependencies. Additionally, summarizer agents must accurately interpret and summarize agent communications to avoid misrepresentations or hallucinations, which could compromise the effectiveness of the entire system.

In summary, selecting an appropriate communication strategy depends on the specific context, objectives, and constraints of the multiagent system. Whether employing structured sequential interactions, parallel exchanges, or hybrid models, each strategy provides distinct advantages and trade-offs, critically influencing the efficiency, responsiveness, and robustness of agent communications.

4.2 Communication Paradigm

Communication paradigms define how information is represented, transmitted, and interpreted among agents in LLM-based multi-agent systems. By utilizing advanced natural language processing capabilities of LLMs, these paradigms enable agents to conduct richer, more context-sensitive interactions than traditional symbolic communication methods. Drawing on the taxonomy proposed by [88], as shown in Fig. 7, three common communication paradigms are distinguished.



Fig. 7 The Communication Paradigms of LLM-MAS

4.2.1 Message Passing

The Message Passing paradigm refers to direct point-to-point or broadcast communication, in which agents explicitly exchange messages containing information, instructions, or requests. These messages typically consist of natural language content augmented with contextual and reasoning-related information, thereby facilitating precise and efficient information dissemination across agents.

A prime example is the simulation of opinion dynamics using networks of LLM-based agents by Chuang et al. [27]. In this scenario, agents use direct messaging to continuously update each other about evolving opinions, thereby maintaining accurate awareness of the collective state and enabling rapid consensus building. Another notable application is GameChat [28], where multiple LLM agents interact via direct message exchanges to achieve safe and socially optimal navigation in constrained environments.

While effective in ensuring clarity and immediacy of interactions, message passing requires robust message handling systems to manage potential overloads and ensure consistency.

4.2.2 Speech Act

The Speech Act paradigm stems from the notion that language serves not only as a medium for information exchange but also as a tool to perform actions. The Speech Act paradigm conceptualizes communication as performative actions where agent utterances are designed to trigger specific actions or state changes within the system. Speech acts typically include instructive, persuasive, or directive components explicitly crafted to influence recipient agent behaviors, dynamically shaping system dynamics based on evolving interaction contexts.

Concretely, speech acts enable agents to steer interactions in contexts that require on-the-fly adaptation, including diplomatic negotiation [61, 69], collaborative reasoning or debate-driven optimization [24], and large-scale software co-engineering workflows [29]. By embedding directive, commissive, or persuasive components into messages, agents can negotiate task allocations, align beliefs, and synchronously coordinate temporal commitments, thereby shaping macrolevel system dynamics as the dialogue unfolds.

Yet this expressive power comes at a cost. Ambiguous force-marking, underspecified contextual frames, or divergent belief models can cause illocutionary misfires: the recipient may infer an unintended goal or act on incomplete preconditions, leading to deadlocks or cascading errors. Mitigating such risks calls for standardized performative taxonomies and explicit grounding protocols—possibly augmented with uncertainty-aware LLM decoding—that allow agents to confirm or renegotiate semantic commitments before executing high-impact actions.

4.2.3 Blackboard

The Blackboard paradigm employs a centralized information repository, where agents collaboratively share, retrieve, and coordinate through published messages or updates. This shared medium acts as a communal workspace, significantly enhancing coordination effectiveness and facilitating a unified understanding among agents about current system states, tasks, or decisions.

This paradigm particularly suits highly coordinated systems like collaborative decision-making or distributed problem-solving, where agents require a shared information pool to align strategies and actions. A typical application example is MetaGPT [4], which effectively leverages the blackboard paradigm by implementing a centralized communication repository where software development agents collaboratively post status updates, code snippets, or issue resolutions. This centralization enables efficient information sharing, coordinated task allocation, and rapid consensus formation, streamlining collaborative development efforts. Similarly, MDTeamGPT [58] demonstrates blackboard usage in medical consultations, where a shared information space ensures medical teams consistently access relevant patient information, diagnostic suggestions, and treatment plans.

While highly beneficial for enhancing information consistency and accessibility, blackboard systems require robust mechanisms to prevent bottlenecks, manage access permissions, and mitigate risks from misinformation or malicious inputs.

In summary, selecting appropriate communication paradigms is crucial for maximizing interaction effectiveness in LLM-based multiagent systems. Each paradigm offers distinct advantages and considerations, tailored to specific interaction scenarios and system requirements. The choice of paradigm significantly influences overall communication coherence, system responsiveness, and the efficacy of collaborative outcomes.

4.3 Communication Object

Communication objects define the entities or targets with which agents interact within an LLM-based multi-agent system. These interactions significantly shape agents' perceptions, decisions, and behaviors. Identifying and clearly defining these communication objects enhances system clarity, enables more targeted interactions, and improves overall coordination and efficiency. As shown in Fig. 8, this section examines four primary communication objects.



Fig. 8 The Communication Objects of LLM-MAS

4.3.1 Communication with Self

Communication with self refers to internal dialogues or reflective processes within agents, enabling them to deliberate, plan, and refine decisions independently [96]. This self-interaction is crucial for agents to update their internal state, manage cognitive resources, and facilitate sophisticated reasoning processes that emulate human-like introspection and problem-solving.

For instance, AgentCoord [50] uses self-communication to iteratively evaluate and refine coordination strategies among multiple agents. Agents internally reflect on past interactions, hypothesize outcomes of potential actions, and update their strategies accordingly. Similarly, FixAgent [71] utilizes self-reflection during debugging tasks, allowing individual agents to internally assess debugging strategies before implementing solutions, thereby significantly enhancing debugging effectiveness and resource management.

However, internal communication requires robust cognitive frameworks within agents to accurately simulate reflective processes, posing challenges in accurately managing agent cognition.

4.3.2 Communication with Other Agents

Communication with other agents involves direct interactions among agents, encompassing exchanges of information, coordination of tasks, or negotiation processes, which exist in the majority of LLM-MAS. Effective inter-agent communication is critical for collaborative problem-solving, conflict resolution, and coordinated decision-making.

MAGIS [49] exemplifies robust inter-agent communication in collaborative software development tasks, where developers, testers, and administrators frequently exchange task-specific messages to streamline software issue resolution. Similarly, AgentFM [76] utilizes structured communication among agents managing database systems, ensuring coordinated responses to failure management and improving system reliability.

Almost all LLM-MAS scenarios involve communication with other agents. Effective inter-agent communication requires sophisticated protocols and mechanisms to ensure synchronization, consistency, and conflict resolution, particularly in large-scale multi-agent systems.

4.3.3 Communication with Environment

Communication with the environment refers to an agent's ability to sense external stimuli and adjust its behavior in real time. Unlike communicating with agents or humans, this modality hinges on parsing raw sensor streams including images, audio, proprioception, or simulator state and converting them into actionable knowledge.

EmbodiedGPT [18] demonstrates environmental communication through multimodal perception, where agents process and respond to sensory inputs like visual and audio data, effectively navigating and interacting within dynamic environments. Similarly, ChatSim [73] incorporates environmental feedback into agent interactions during autonomous driving simulations, enabling agents to refine their behaviors based on real-time environmental changes and conditions.

Robust environment communication thus demands accurate, low-latency sensor fusion, continual grounding of textual reasoning in non-linguistic data, and safety guards against perception errors or out-of-distribution inputs. Addressing these challenges is essential for deploying LLM-MAS in dynamic, high-stakes settings such as embodied assistance, industrial automation, or intelligent transportation.

4.3.4 Communication with Human

Communication with humans involves direct interactions between agents and human users or participants. This interaction layer adds complexity to multi-agent systems by requiring agents to understand, interpret, and appropriately respond to human-generated inputs, commands, or feedback, maintaining effective and natural interactions.

PeerGPT [72] effectively illustrates human-agent communication in collaborative educational scenarios, where agents function as moderators or participants interacting dynamically with children. Agents interpret children's verbal inputs and physical actions, continuously refining their responses to enhance learning outcomes and maintain engagement. Additionally, MedAgents [59] exemplifies human-agent interaction in medical consultations, where agents collaboratively interact with medical professionals to support diagnosis, treatment planning, and patient care coordination.

These applications highlight three challenges: robust natural-language understanding across diverse user populations, integration of affective and situational signals to maintain rapport, and stringent safety and ethical requirements concerning privacy, bias, and accountability. Addressing these challenges is critical for deploying LLM-MAS that can communicate with humans in a trustworthy and effective manner.

In summary, clearly defining and managing communication objects is essential for optimizing agent interactions in LLM-MAS. Effective management of these interactions significantly influences the system's adaptability, responsiveness, and overall operational effectiveness.

4.4 Communication Content

Communication content specifies the type and nature of information exchanged between agents, influencing their interactions, understanding, and subsequent actions. As shown in Fig. 9, this section categorizes communication content into Explicit and Implicit forms, with further subdivisions to enhance clarity and provide detailed insights into their application contexts.

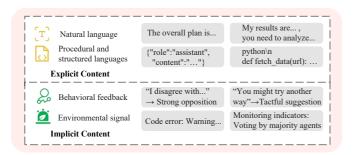


Fig. 9 The Communication Contents of LLM-MAS

4.4.1 Explicit communication

Explicit communication entails direct information exchange with clearly defined and easily interpretable meaning. Explicit communication can be divided into two forms:

• Natural Language.

Explicit communication in the form of natural language involves direct verbal exchanges articulated in human-readable text or spoken formats. This type of communication leverages the advanced natural language processing capabilities of LLMs, allowing agents to communicate clearly, flexibly, and contextually.

For example, generative agents in sandbox environments [63] frequently utilize natural language communication to negotiate, plan, or resolve conflicts, mirroring complex human interactions. Moreover, agents in platforms like AgentCoord [50] employ natural language to articulate strategic decisions clearly, ensuring smooth and effective coordination among agents. The flexibility and expressiveness of natural language enhance the quality of interactions but require sophisticated parsing capabilities to avoid ambiguities or misunderstandings.

• Code and Structured Data.

Communication through code and structured data involves precise, unambiguous exchanges, typically formatted in standardized data structures or procedural languages. This form of explicit communication is essential for tasks requiring high accuracy and clarity, such as detailed instructions, algorithmic descriptions, or structured data exchanges.

For instance, MAGIS [49] utilizes structured code and data exchanges among software development agents to streamline issue tracking and code management processes. Similarly, AutoData [36] applies structured data communication for open web data collection, ensuring efficient and accurate data aggregation and analysis. Structured communication effectively minimizes misinterpretations but demands strict adherence to predefined data standards and formats.

4.4.2 Implicit communication.

Implicit communication occurs when agents convey information indirectly, through their actions or environmental cues, rather than through explicit statements. Implicit communication relies on agents interpret-

ing contextual cues or feedback. Implicit communication can also be divided into two forms:

· Behavioral Feedback.

Implicit communication through behavioral feedback involves indirect information exchanges inferred from agent actions or interactions. Instead of explicit verbal cues, agents communicate intentions or feedback implicitly through observable behaviors, strategy shifts, or adaptive responses. Such signals can convey intent, commitment, or private information while preserving strategic stealth.

In diplomatic simulations like Richelieu [69], agent behaviors implicitly communicate negotiation positions and strategies, influencing the negotiation outcomes indirectly. Similarly, Flooding simulations [47] demonstrate implicit behavioral feedback, where agent strategies dynamically adjust based on the evolving behaviors of peers, effectively communicating strategic adjustments without explicit verbalization. Although powerful, behavioral feedback requires accurate interpretation mechanisms to ensure the correct inference of implicit signals, otherwise it may cause misjudgment or over-interpretation, resulting in impaired system function.

• Environmental Signal.

Environmental signals serve as another implicit communication channel, where changes or conditions in the operational context indirectly influence agent decisions and behaviors. Agents interpret and respond to these signals to dynamically adapt their actions.

For example, ChatSim [73] integrates environmental signals such as real-time traffic or weather conditions in autonomous driving simulations, guiding agent navigation decisions implicitly. Likewise, agents in EcoLANG [70] interpret economic indicators and environmental signals to adjust consumption and investment behaviors dynamically. Effective utilization of environmental signals depends heavily on the agents' sensitivity and responsiveness to subtle contextual changes.

In summary, clearly distinguishing and effectively managing explicit and implicit communication content is crucial for enhancing interaction accuracy, adaptability, and overall efficacy in LLM-MAS.

■ 5 Challenges and Opportunities

As LLM-MAS continue to garner increasing attention in both research and application domains, their further development faces several significant challenges and emerging opportunities. We analyze several key challenges and research directions based on the article's content.

5.1 Optimizing the System Design

The communication architecture is the foundational component of LLM-MAS. As task complexity increases, traditional communication architectures may no longer suffice. Therefore, the design of hybrid architectures is expected to be a key focus of future research. With more complex structures, the number of agents increases, leading to greater demands on computational resources. Therefore, a major challenge lies in developing communication paradigms that are both efficient and scalable. Meanwhile, how to optimize the allocation of computational resources also needs to be considered. Concurrently, the increasing volume of internal system information poses another challenge. Ensuring that agents correctly interpret and understand this information,

while minimizing the risk of hallucinations or misunderstandings, will be a crucial area of investigation.

5.2 Advancing Research on Agent Competition

In a competitive environment, agents can develop more complex strategies, improve decision-making, and promote innovative behaviors by employing techniques such as game theory. However, a key challenge lies in balancing competition and cooperation, as excessive competition may lead to inefficiency or instability. Future research can focus on finding the optimal balance between competition and cooperation, developing scalable competition strategies, and exploring how to safely and effectively integrate competition into real-world applications.

5.3 Unified Communication Protocol

The rapid emergence and deployment of multiple new communication protocols such as MCP, A2A, ANP, ACP, AITP, and AConP in LLM-MAS underscore the field's dynamism and growth. However, this proliferation also brings critical challenges. One significant issue is functional redundancy, as different protocols often overlap in terms of capabilities such as secure communication, context management, and agent discovery. This redundancy can lead to unnecessary complexity, resource wastage, and increased difficulty in protocol management.

Moreover, the lack of interoperability among existing protocols poses substantial barriers. Different agent groups employing distinct protocols cannot seamlessly communicate or collaborate, significantly hindering the scalability and integration of multi-agent systems. This situation mirrors early-stage internet communication challenges, which were eventually resolved through standardized protocols like HTTPS.

Therefore, the development and adoption of a unified, standardized communication protocol for LLM-MAS is imperative. Such a protocol would provide foundational interoperability, enhance security, simplify integration, and significantly reduce the complexity inherent in managing multiple disparate systems. By achieving a consensus-driven standard akin to HTTPS, LLM-MAS can more effectively harness the collective intelligence and collaborative potential of agents, thereby driving further innovation, reliability, and widespread adoption across diverse application domains.

5.4 Multimodal Communication

With the development of large multimodal models, agents in LLM-MAS should not be limited to text-based communication. Communication of multimodal content (text, images, audio, and video) should also be considered. This expansion into multimodal content enables more natural and context-aware interactions, thereby enhancing agents' adaptability and decision-making capabilities. However, there are some challenges to integrating multimodal content. A major issue is how to effectively present and coordinate different modalities in a coherent way that is comprehensible to all agents. In addition, agents not only have to process these different modalities, but also communicate them effectively to one another. Future research should focus on improving the fusion of multimodal data and designing stronger agents in key components for handling multimodal content.

5.5 Communication Security

As LLM-MAS migrate into safety-critical domains, safeguarding the confidentiality, integrity, and authenticity of inter-agent messages is indispensable. Recent studies [47,97,98] demonstrate that adversaries can mount man-in-the-middle, data-tampering, and spoofing attacks, resulting in damage cascading rapidly through the system. Hence, defence techniques originally designed for standalone LLMs [99,100] must be embedded within the communication layer itself. Preventing eavesdropping and forgery in decentralized, dynamic topologies where agents may join or leave at will requires cryptographically grounded protocols that combine end-to-end encryption, fine-grained authentication, adaptive key management, and provenance tracking. Developing such adaptive secure-communication frameworks will be pivotal for deploying LLM-MAS in high-stakes settings such as cooperative autonomous driving and clinical decision support, where even transient message corruption can have cascading real-world consequences.

5.6 Benchmarks and Evaluation

The rapid diffusion of LLM-MAS across software engineering, game-playing, and social-simulation tasks has outpaced the development of rigorous evaluation suites. Existing datasets such as MultiAgentBench and RealWorldBench [101, 102] cover a handful of cooperative scenarios, but fall short of spanning heterogeneous domains, interaction paradigms, or agent-population scales.

Current leaderboards also remain agent-centric: they report peragent task accuracy or reward but rarely capture system-level properties, including coordination efficiency, communication bandwidth and latency, robustness to stale or deceptive messages, and group-level fairness and safety. Without these dimensions, evaluations cannot distinguish architectures that merely aggregate strong single agents from those that yield genuinely emergent collaboration.

We therefore advocate a next-generation benchmark suite that spans cooperation, competition, and mixed-motive settings and reports a multi-granular metric set from individual competence to collective utility to provide a holistic portrait of LLM-MAS performance.

■ 6 Conclusion

In this survey, we have presented a communication-centric framework for understanding LLM-MAS, emphasizing how effective communication shapes system performance. By distinguishing between system-level communication and system-internal communication, we system-atically explored critical components, including architectures, communication goals, protocols, strategies, paradigms, objects, and content. The significant impacts of these components on the efficiency, scalability, and adaptability of LLM-MAS are discussed in detail. We also discuss challenges and future opportunities. Key challenges identified include interoperability, multimodal integration, and security. Future research directions should focus on addressing these issues, optimizing system designs, developing unified protocols, and establishing comprehensive benchmarks. We expect this communication-centric perspective to inform and inspire ongoing research, driving further development of LLM-MAS.

■ Acknowledgement

This research is supported by the National Natural Science Foundation of China (No.62272025, No.U22B2021 and No.62362048)

■ Competing Interest

The authors declare that they have no competing interests or financial conflicts to disclose.

■ References

- [1] Wang L, Ma C, Feng X, Zhang Z, Yang H, Zhang J, Chen Z, Tang J, Chen X, Lin Y, others . A survey on large language model based autonomous agents. Frontiers of Computer Science, 2024, 18(6): 186345
- [2] Talebirad Y, Nadiri A. Multi-agent collaboration: Harnessing the power of intelligent llm agents. arXiv preprint arXiv:2306.03314, 2023
- [3] Cai J, Li J, Zhang M, Li M, Wang C S, Tei K. Language evolution for evading social media regulation via llm-based multi-agent simulation. In: 2024 IEEE Congress on Evolutionary Computation (CEC). 2024, 1–10
- [4] Hong S, Zheng X, Chen J, Cheng Y, Wang J, Zhang C, Wang Z, Yau S K S, Lin Z, Zhou L, others . Metagpt: Meta programming for multi-agent collaborative framework. arXiv preprint arXiv:2308.00352, 2023, 3(4): 6
- [5] Nie G, Zhi R, Yan X, Du Y, Zhang X, Chen J, Zhou M, Chen H, Li T, Cheng Z, others . A hybrid multi-agent conversational recommender system with llm and search engine in e-commerce. In: Proceedings of the 18th ACM Conference on Recommender Systems. 2024, 745–747
- [6] Li X, Wang S, Zeng S, Wu Y, Yang Y. A survey on Ilm-based multi-agent systems: workflow, infrastructure, and challenges. Vicinagearth, 2024, 1(1): 9
- [7] Guo T, Chen X, Wang Y, Chang R, Pei S, Chawla N V, Wiest O, Zhang X. Large language model based multi-agents: A survey of progress and challenges. arXiv preprint arXiv:2402.01680, 2024
- [8] Han S, Zhang Q, Yao Y, Jin W, Xu Z, He C. Llm multiagent systems: Challenges and open problems. arXiv preprint arXiv:2402.03578, 2024
- [9] Gao C, Lan X, Li N, Yuan Y, Ding J, Zhou Z, Xu F, Li Y. Large language models empowered agent-based modeling and simulation: A survey and perspectives. Humanities and Social Sciences Communications, 2024, 11(1): 1–24
- [10] Jin H, Huang L, Cai H, Yan J, Li B, Chen H. From llms to llm-based agents for software engineering: A survey of current, challenges and future. arXiv preprint arXiv:2408.02479, 2024
- [11] Liu J, Wang K, Chen Y, Peng X, Chen Z, Zhang L, Lou Y. Large language model-based agents for software engineering: A survey. arXiv preprint arXiv:2409.02977, 2024
- [12] Shannon C E. A mathematical theory of communication. The Bell system technical journal, 1948, 27(3): 379–423
- [13] Smith R G. The contract net protocol: High-level communication and control in a distributed problem solver. IEEE Transactions on computers, 1980, 29(12): 1104–1113

- [14] Cheng Y, Zhang C, Zhang Z, Meng X, Hong S, Li W, Wang Z, Wang Z, Yin F, Zhao J, others . Exploring large language model based intelligent agents: Definitions, methods, and prospects. arXiv preprint arXiv:2401.03428, 2024
- [15] Zhang Q, Chen S, Bei Y, Yuan Z, Zhou H, Hong Z, Dong J, Chen H, Chang Y, Huang X. A survey of graph retrieval-augmented generation for customized large language models. arXiv preprint arXiv:2501.13958, 2025
- [16] Chen S, Zhang Q, Dong J, Hua W, Li Q, Huang X. Entity alignment with noisy annotations from large language models. arXiv preprint arXiv:2405.16806, 2024
- [17] Qin Y, Liang S, Ye Y, Zhu K, Yan L, Lu Y, Lin Y, Cong X, Tang X, Qian B, others . Toolllm: Facilitating large language models to master 16000+ real-world apis. arXiv preprint arXiv:2307.16789, 2023
- [18] Mu Y, Zhang Q, Hu M, Wang W, Ding M, Jin J, Wang B, Dai J, Qiao Y, Luo P. Embodiedgpt: Vision-language pre-training via embodied chain of thought. Advances in Neural Information Processing Systems, 2023, 36: 25081–25094
- [19] Wooldridge M. An introduction to multiagent systems. John wiley & sons, 2009
- [20] Oliehoek F A, Amato C, others . A concise introduction to decentralized POMDPs. volume 1. Springer, 2016
- [21] Hu J, Bhowmick P, Jang I, Arvin F, Lanzon A. A decentralized cluster formation containment framework for multirobot systems. IEEE Transactions on Robotics, 2021, 37(6): 1936–1955
- [22] Ulmer D, Mansimov E, Lin K, Sun J, Gao X, Zhang Y. Bootstrapping llm-based task-oriented dialogue agents via self-talk. arXiv preprint arXiv:2401.05033, 2024
- [23] Abdullin Y, Molla-Aliod D, Ofoghi B, Yearwood J, Li Q. Synthetic dialogue dataset generation using llm agents. arXiv preprint arXiv:2401.17461, 2024
- [24] Du Y, Li S, Torralba A, Tenenbaum J B, Mordatch I. Improving factuality and reasoning in language models through multiagent debate. In: Forty-first International Conference on Machine Learning. 2023
- [25] Hsu C J, Buffelli D, McGowan J, Liao F T, Chen Y C, Vakili S, Shiu D s. Group think: Multiple concurrent reasoning agents collaborating at token level granularity. arXiv preprint arXiv:2505.11107, 2025
- [26] Huang J t, Li E J, Lam M H, Liang T, Wang W, Yuan Y, Jiao W, Wang X, Tu Z, Lyu M R. How far are we on the decision-making of llms? evaluating llms' gaming ability in multi-agent environments. arXiv preprint arXiv:2403.11807, 2024
- [27] Chuang Y S, Goyal A, Harlalka N, Suresh S, Hawkins R, Yang S, Shah D, Hu J, Rogers T T. Simulating opinion dynamics with networks of llm-based agents. arXiv preprint arXiv:2311.09618, 2023
- [28] Mahadevan V, Zhang S, Chandra R. Gamechat: Multi-Ilm dialogue for safe, agile, and socially optimal multi-agent navigation in constrained environments. arXiv preprint arXiv:2503.12333, 2025
- [29] Qian C, Liu W, Liu H, Chen N, Dang Y, Li J, Yang C, Chen W, Su Y, Cong X, others . Chatdev: Communicative agents for software development. arXiv preprint arXiv:2307.07924, 2023

- [30] Zeng Y, Wu Y, Zhang X, Wang H, Wu Q. Autodefense: Multi-agent llm defense against jailbreak attacks. arXiv preprint arXiv:2403.04783, 2024
- [31] Tang Z, Wang R, Chen W, Wang K, Liu Y, Chen T, Lin L. Towards causalgpt: A multi-agent approach for faithful knowledge reasoning via promoting causal consistency in llms. arXiv preprint arXiv:2308.11914, 2023
- [32] Ishibashi Y, Nishimura Y. Self-organized agents: A llm multiagent framework toward ultra large-scale code generation and optimization. arXiv preprint arXiv:2404.02183, 2024
- [33] Yu Y, Yao Z, Li H, Deng Z, Jiang Y, Cao Y, Chen Z, Suchow J, Cui Z, Liu R, others . Fincon: A synthesized llm multi-agent system with conceptual verbal reinforcement for enhanced financial decision making. Advances in Neural Information Processing Systems, 2024, 37: 137010–137045
- [34] Wang S, Long Z, Fan Z, Wei Z, Huang X. Benchmark self-evolving: A multi-agent framework for dynamic llm evaluation. arXiv preprint arXiv:2402.11443, 2024
- [35] Zhang Y, Sun R, Chen Y, Pfister T, Zhang R, Arik S. Chain of agents: Large language models collaborating on long-context tasks. Advances in Neural Information Processing Systems, 2024, 37: 132208–132237
- [36] Ma T, Qian Y, Zhang Z, Wang Z, Qian X, Bai F, Ding Y, Luo X, Zhang S, Murugesan K, others . Autodata: A multi-agent system for open web data collection. arXiv preprint arXiv:2505.15859, 2025
- [37] Yang T, Feng P, Guo Q, Zhang J, Ning J, Wang X, Mao Z. Autohma-llm: Efficient task coordination and execution in heterogeneous multi-agent systems using hybrid large language models. IEEE Transactions on Cognitive Communications and Networking, 2025
- [38] Wang S, Zhang G, Yu M, Wan G, Meng F, Guo C, Wang K, Wang Y. G-safeguard: A topology-guided security lens and treatment on llm-based multi-agent systems. arXiv preprint arXiv:2502.11127, 2025
- [39] Li H, Xu T, Chang E, Wen Q. Knowledge tagging with large language model based multi-agent system. In: Proceedings of the AAAI Conference on Artificial Intelligence. 2025, 28775–28782
- [40] Kalyuzhnaya A, Mityagin S, Lutsenko E, Getmanov A, Aksenkin Y, Fatkhiev K, Fedorin K, Nikitin N O, Chichkova N, Vorona V, others . Llm agents for smart city management: Enhancing decision support through multi-agent ai systems. Smart Cities (2624-6511), 2025, 8(1)
- [41] Zhang K, Zhang C, Wang C, Zhang C, Wu Y, Xing Z, Liu Y, Li Q, Peng X. Logiagent: Automated logical testing for rest systems with llm-based multi-agents. arXiv preprint arXiv:2503.15079, 2025
- [42] Lei B, Zhang Y, Zuo S, Payani A, Ding C. Macm: Utilizing a multi-agent system for condition mining in solving complex mathematical problems. arXiv preprint arXiv:2404.04735, 2024
- [43] Islam M A, Ali M E, Parvez M R. Codesim: Multi-agent code generation and problem solving through simulation-driven planning and debugging. arXiv preprint arXiv:2502.05664, 2025
- [44] Shen M, Shu R, Pratik A, Gung J, Ge Y, Sunkara M, Zhang Y. Optimizing llm-based multi-agent system with textual feedback: A

- case study on software development. arXiv preprint arXiv:2505.16086, 2025
- [45] Hu Y, Cai Y, Du Y, Zhu X, Liu X, Yu Z, Hou Y, Tang S, Chen S. Self-evolving multi-agent collaboration networks for software development. arXiv preprint arXiv:2410.16946, 2024
- [46] Wang Z, Moriyama S, Wang W Y, Gangopadhyay B, Takamatsu S. Talk structurally, act hierarchically: A collaborative framework for llm multi-agent systems. arXiv preprint arXiv:2502.11098, 2025
- [47] Ju T, Wang Y, Ma X, Cheng P, Zhao H, Wang Y, Liu L, Xie J, Zhang Z, Liu G. Flooding spread of manipulated knowledge in llm-based multi-agent communities. arXiv preprint arXiv:2407.07791, 2024
- [48] Wu D, Shi H, Sun Z, Liu B. Deciphering digital detectives: Understanding llm behaviors and capabilities in multi-agent mystery games. arXiv preprint arXiv:2312.00746, 2023
- [49] Tao W, Zhou Y, Wang Y, Zhang W, Zhang H, Cheng Y. Magis: Llm-based multi-agent framework for github issue resolution. Advances in Neural Information Processing Systems, 2024, 37: 51963–51993
- [50] Pan B, Lu J, Wang K, Zheng L, Wen Z, Feng Y, Zhu M, Chen W. Agentcoord: Visually exploring coordination strategy for llm-based multi-agent collaboration. arXiv preprint arXiv:2404.11943, 2024
- [51] Chen G, Dong S, Shu Y, Zhang G, Sesay J, Karlsson B F, Fu J, Shi Y. Autoagents: A framework for automatic agent generation. arXiv preprint arXiv:2309.17288, 2023
- [52] Qian C, Dang Y, Li J, Liu W, Xie Z, Wang Y, Chen W, Yang C, Cong X, Che X, others . Experiential co-learning of software-developing agents. arXiv preprint arXiv:2312.17025, 2023
- [53] Zhang Z, Zhang-Li D, Yu J, Gong L, Zhou J, Hao Z, Jiang J, Cao J, Liu H, Liu Z, others . Simulating classroom education with llm-empowered agents. arXiv preprint arXiv:2406.19226, 2024
- [54] Fan Y, Xue K, Li Z, Zhang X, Ruan T. An Ilm-based framework for biomedical terminology normalization in social media via multi-agent collaboration. In: Proceedings of the 31st International Conference on Computational Linguistics. 2025, 10712–10726
- [55] Ma W, Zhang H, Yang I, Ji S, Chen J, Hashemi F, Mohole S, Gearey E, Macy M, Hassanpour S, others . Communication makes perfect: Persuasion dataset construction via multi-llm communication. In: Proceedings of the 2025 Conference of the Nations of the Americas Chapter of the Association for Computational Linguistics: Human Language Technologies (Volume 1: Long Papers). 2025, 4017–4045
- [56] Zhang Q W, Li F, Wang J, Qiao L, Yu Y, Yin D, Sun X. Factguard: Leveraging multi-agent systems to generate answerable and unanswerable questions for enhanced long-context llm extraction. arXiv preprint arXiv:2504.05607, 2025
- [57] Luo Y, Feng Y, Xu J, Tasca P, Liu Y. Llm-powered multi-agent system for automated crypto portfolio management. arXiv preprint arXiv:2501.00826, 2025
- [58] Chen K, Li X, Yang T, Wang H, Dong W, Gao Y. Mdteamgpt: A self-evolving llm-based multi-agent framework for multi-disciplinary team medical consultation. arXiv preprint arXiv:2503.13856, 2025
- [59] Tang X, Zou A, Zhang Z, Li Z, Zhao Y, Zhang X, Cohan A,

- Gerstein M. Medagents: Large language models as collaborators for zero-shot medical reasoning. arXiv preprint arXiv:2311.10537, 2023
- [60] Qiao T, Walker C, Cunningham C, Koh Y S. Thematic-lm: A llm-based multi-agent system for large-scale thematic analysis. In: Proceedings of the ACM on Web Conference 2025. 2025, 649–658
- [61] Moghimifar F, Li Y F, Thomson R, Haffari G. Modelling political coalition negotiations using llm-based agents. arXiv preprint arXiv:2402.11712, 2024
- [62] Wang S, Liu C, Zheng Z, Qi S, Chen S, Yang Q, Zhao A, Wang C, Song S, Huang G. Boosting Ilm agents with recursive contemplation for effective deception handling. In: Findings of the Association for Computational Linguistics ACL 2024. 2024, 9909–9953
- [63] Park J S, O'Brien J, Cai C J, Morris M R, Liang P, Bernstein M S. Generative agents: Interactive simulacra of human behavior. In: Proceedings of the 36th annual acm symposium on user interface software and technology. 2023. 1–22
- [64] Piatti G, Jin Z, Kleiman-Weiner M, Schölkopf B, Sachan M, Mihalcea R. Cooperate or collapse: Emergence of sustainable cooperation in a society of llm agents. Advances in Neural Information Processing Systems, 2024, 37: 111715–111759
- [65] Shengbin Yue S, Huang T, Jia Z, Wang S, Liu S, Song Y, Huang X J, Wei Z. Multi-agent simulator drives language models for legal intensive interaction. In: Findings of the Association for Computational Linguistics: NAACL 2025. 2025, 6537–6570
- [66] Sreedhar K, Cai A, Ma J, Nickerson J V, Chilton L B. Simulating cooperative prosocial behavior with multi-agent llms: Evidence and mechanisms for ai agents to inform policy decisions. In: Proceedings of the 30th International Conference on Intelligent User Interfaces. 2025, 1272–1286
- [67] Dai G, Zhang W, Li J, Yang S, Rao S, Caetano A, Sra M, others . Artificial leviathan: Exploring social evolution of llm agents through the lens of hobbesian social contract theory. arXiv preprint arXiv:2406.14373, 2024
- [68] Li N, Gao C, Li M, Li Y, Liao Q. Econagent: large language model-empowered agents for simulating macroeconomic activities. arXiv preprint arXiv:2310.10436, 2023
- [69] Guan Z, Kong X, Zhong F, Wang Y. Richelieu: Self-evolving llm-based agents for ai diplomacy. Advances in Neural Information Processing Systems, 2024, 37: 123471–123497
- [70] Mou X, Qian C, Liu W, Huang X, Wei Z. Ecolang: Efficient and effective agent communication language induction for social simulation. arXiv preprint arXiv:2505.06904, 2025
- [71] Lee C, Xia C S, Yang L, Huang J t, Zhu Z, Zhang L, Lyu M R. A unified debugging approach via llm-based multi-agent synergy. arXiv preprint arXiv:2404.17153, 2024
- [72] Liu J, Yao Y, An P, Wang Q. Peergpt: Probing the roles of Ilmbased peer agents as team moderators and participants in children's collaborative learning. In: Extended Abstracts of the CHI Conference on Human Factors in Computing Systems. 2024, 1–6
- [73] Wei Y, Wang Z, Lu Y, Xu C, Liu C, Zhao H, Chen S, Wang Y. Editable scene simulation for autonomous driving via collaborative llm-agents. In: Proceedings of the IEEE/CVF Conference on

- Computer Vision and Pattern Recognition. 2024, 15077–15087
- [74] Ocker F, Tanneberg D, Eggert J, Gienger M. Tulip agent–enabling llm-based agents to solve tasks using large tool libraries. arXiv preprint arXiv:2407.21778, 2024
- [75] Kim K, Lee S, Huang K H, Chan H P, Li M, Ji H. Can llms produce faithful explanations for fact-checking? towards faithful explainable fact-checking via multi-agent debate. arXiv preprint arXiv:2402.07401, 2024
- [76] Zhang L, Zhai Y, Jia T, Huang X, Duan C, Li Y. Agentfm: Role-aware failure management for distributed databases with llm-driven multi-agents. arXiv preprint arXiv:2504.06614, 2025
- [77] Ronanki K. Facilitating trustworthy human-agent collaboration in llm-based multi-agent system oriented software engineering. arXiv preprint arXiv:2505.04251, 2025
- [78] Zhang Y, Hao J, Wang Z, Sheng H, Zeng W. Facilitating video story interaction with multi-agent collaborative system. arXiv preprint arXiv:2505.03807, 2025
- [79] Pei C, Wang Z, Liu F, Li Z, Liu Y, He X, Kang R, Zhang T, Chen J, Li J, others . Flow-of-action: Sop enhanced llm-based multi-agent system for root cause analysis. arXiv preprint arXiv:2502.08224, 2025
- [80] Wang T, Zhan Y, Lian J, Hu Z, Yuan N J, Zhang Q, Xie X, Xiong H. Llm-powered multi-agent framework for goal-oriented learning in intelligent tutoring system. arXiv preprint arXiv:2501.15749, 2025
- [81] Zhang Y, Yang X, Feng S, Wang D, Zhang Y, Song K. Can llms beat humans in debating? a dynamic multi-agent framework for competitive debate. arXiv preprint arXiv:2408.04472, 2024
- [82] Zhang R, Eger S. Llm-based multi-agent poetry generation in non-cooperative environments. arXiv preprint arXiv:2409.03659, 2024
- [83] Wu Z, Peng R, Zheng S, Liu Q, Han X, Kwon B I, Onizuka M, Tang S, Xiao C. Shall We Team Up: Exploring Spontaneous Cooperation of Competing LLM Agents. Papers 2402.12327, arXiv.org, February 2024
- [84] Chen B, Li G, Lin X, Wang Z, Li J. Blockagents: Towards byzantine-robust llm-based multi-agent coordination via blockchain. In: Proceedings of the ACM Turing Award Celebration Conference-China 2024. 2024, 187–192
- [85] Xu Q, Tian Z, Wu H, Huang Z, Song Y, Liu F, Li D. Learn to disguise: Avoid refusal responses in llm's defense via a multi-agent attacker-disguiser game. arXiv preprint arXiv:2404.02532, 2024
- [86] Yim Y, Chan C, Shi T, Deng Z, Fan W, Zheng T, Song Y. Evaluating and enhancing llms agent based on theory of mind in guandan: A multi-player cooperative game under imperfect information. arXiv preprint arXiv:2408.02559, 2024
- [87] Liu Y, Liu Y, Zhang X, Chen X, Yan R. The truth becomes clearer through debate! multi-agent systems with large language models unmask fake news. arXiv preprint arXiv:2505.08532, 2025
- [88] Dorri A, Kanhere S S, Jurdak R. Multi-agent systems: A survey. Ieee Access, 2018, 6: 28573–28593
- [89] Model Context Protocol . Introduction to model context protocol (mcp). https://modelcontextprotocol.io/introduction, 2024. Accessed: May 2025

- [90] Google . Agent2agent (a2a) protocol. https://google.github.io/A2A/, 2024. Accessed: May 2025
- [91] Agent Network Protocol Contributors. Agent network protocol official website. https://agent-network-protocol.com/, 2024. Accessed: May 2025
- [92] Ehtesham A, Singh A, Gupta G K, Kumar S. A survey of agent interoperability protocols: Model context protocol (mcp), agent communication protocol (acp), agent-to-agent protocol (a2a), and agent network protocol (anp). arXiv preprint arXiv:2505.02279, 2025
- [93] Linux Foundation AI and LBM Data . Acp: Agent communication protocol. https://github.com/orgs/i-am-bee/discussions/284, 2025. Accessed: May 2025
- [94] NEAR. Aitp: Agent interaction & transaction protocol. https://aitp.dev/, 2025. Accessed: May 2025
- [95] Galileo Cisco and Langchain. Agent connect protocol. https://spec.acp.agntcy.org/, 2025. Accessed: May 2025
- [96] Yao S, Zhao J, Yu D, Du N, Shafran I, Narasimhan K, Cao Y. React: Synergizing reasoning and acting in language models. In: International Conference on Learning Representations (ICLR). 2023 [97] He P, Lin Y, Dong S, Xu H, Xing Y, Liu H. Red-teaming

- Ilm multi-agent systems via communication attacks. arXiv preprint arXiv:2502.14847, 2025
- [98] Zhou Z, Li Z, Zhang J, Zhang Y, Wang K, Liu Y, Guo Q. Corba: Contagious recursive blocking attacks on multi-agent systems based on large language models. arXiv preprint arXiv:2502.14529, 2025
- [99] Zou A, Phan L, Wang J, Duenas D, Lin M, Andriushchenko M, Kolter J Z, Fredrikson M, Hendrycks D. Improving alignment and robustness with circuit breakers. In: The Thirty-eighth Annual Conference on Neural Information Processing Systems. 2024
- [100] Jain N, Schwarzschild A, Wen Y, Somepalli G, Kirchenbauer J, Chiang P y, Goldblum M, Saha A, Geiping J, Goldstein T. Baseline defenses for adversarial attacks against aligned language models. arXiv preprint arXiv:2309.00614, 2023
- [101] Zhu K, Du H, Hong Z, Yang X, Guo S, Wang Z, Wang Z, Qian C, Tang X, Ji H, others . Multiagentbench: Evaluating the collaboration and competition of llm agents. arXiv preprint arXiv:2503.01935, 2025 [102] Geng L, Chang E Y. Realm-bench: A real-world planning benchmark for llms and multi-agent systems. arXiv preprint arXiv:2502.18836, 2025