사이버범죄 수사 추론 에이전트를 위한 MCP 기반 도구 연동 플랫폼 개발

김민수, 김성섭, 권영민, 이승우*

한국전자기술연구원

{mskim92, sskim, ymkwon, seungwoo.lee*}@keti.re.kr

MCP-based Tool Integration Platform for Reasoning Agents in Cybercrime Investigation

Minsu Kim, Seongseop Kim, Youngmin Kwon, Seungwoo Lee

Korea Electronics and Technology Institute (KETI)

요 약

사이버범죄 수법의 다양화 및 고도화로 인해 수사관의 범죄수사 과정을 보조하기 위한 인공지능 기반 수사 추론 에이전트의 수요가 증가하고 있다. 기존의 수사 지원 시스템은 단일 도구 중심의 분석에 한정되어 있기 때문에 사건 장소의 변동이 크고 인물 관계가 복잡한 사이버범죄 수사 과정에서 다양한 분석·추론 도구들을 통합적으로 활용하기 어려운 한계가 있다. 본 논문에서는 사이버범죄 수사 추론 에이전트를 위한 MCP (Model Context Protocol) 기반 도구 연동 플랫폼을 제안한다. 제안하는 플랫폼은 도구 API를 통합 및 관리하고, 수사 추론 에이전트가 현재 상황에서 필요한 도구를 선택하여 실행하도록 지원하며, 수사 추론 에이전트와 도구 간의 확장 가능한 연동 아키텍처를 제공한다.

Ⅰ. 서 론

산업 및 사회 전반의 디지털 전환 가속화로 인해 사이버범죄 발생 건수가 지속해서 증가하고 있다. 사이버범죄는 비대면 특성과 투자 사기, 물품 거래 사기 등 다양한 범죄 유형이 존재하기 때문에 수사 난이도가 높다 [1]. 이에 따라 수사관의 용의자 특정 및 추적을 보조하기 위한 인공지능 기반 수사 추론이 주목받고 있다 [2]. 수사 추론은 대형 언어모델 등 추론 능력을 부여할 수 있는 모델을 에이전트로 활용하며, 디지털 증거 및 단서를 분석하여 사실관계를 요약하고 범죄 전모를 재구성함으로써 수사 방향을 결정하는 기술을 의미한다.

사이버범죄는 사이버 공간에서 행해지는 범죄로, 웹사이트, SNS, 메신저 앱 등 다양한 온라인 플랫폼을 매개로 한다 [3]. 이와 같이 복잡한 디지털 환경에서 발생하는 특성 때문에 사이버범죄에 대한 수사 추론은 다수의 분석·추론 도구를 통합하여 활용할 필요가 있다. 그러나, 개별 분석·추론 도구는 서로 다른 API 구조와 데이터 형식을 사용하기 때문에 수사 추론 에이전트의 도구 통합에 어려움이 있다. 따라서 도구 통합 및 연계를 위한 표준 프로토콜의 도입이 필요하며, 최근 MCP (Model Context Protocol)가 해결 방안으로 제시되고 있다. 에이전트와 외부 도구가 상호작용할 수 있도록 지원하는 표준 프로토콜인 MCP는 JSON-RPC 메시징 시스템을 사용하여 일관된 인터페이스를 제공한다. 수사 추론 에이전트는 MCP를 통해 네트워크 분석, 인물 관계 분석 등 다양한 분석·추론 도구를 표준화된 방식으로 연계할 수 있다.

본 논문은 사이버범죄 수사 추론 에이전트를 위한 MCP 기반 도구 연동 플랫폼을 제안한다. 제안하는 플랫폼은 다수의 도구에 대한 동적 연결 및 기능 등록을 지원한다. 기능 등록이 완료된 도구의 API 정보는 플랫폼이 관리하며, 수사 추론 에이전트에게 호출 정보가 제공된다. 수사 추론 에이전트는 직접 질의 혹은 핵심 키워드를 플랫폼으로 전달하여 현재 상황에 적절한 도구를 선택 및 실행한다.

Ⅱ. 관련 연구

기존의 에이전트 도구 연동 기술은 정적인 연결 방식을 사용하기 때문에 에이전트가 학습된 시점 이후의 최신 정보를 반영하는 것과 외부 시스템과의 연결이 어려운 문제가 있다. 따라서 에이전트가 필요한 도구를 사용하도록 하고, 원활한 작업 수행을 지원할 수 있는 표준 연동 프로토콜의 필요성이 커지게 되었다.

Anthropic에서 제안한 공개 표준인 MCP는 JSON-RPC 메시징을 통해 인공지능 어플리케이션과 외부 도구 간의 상호작용을 표준화한다. MCP는 호스트, 서버, 그리고 클라이언트의 3계층 아키텍처를 채택하여 확장성과 유연성을 제공한다 [4]. 호스트는 사용자 작업 환경을 의미하며, 서버는 도구의 기능을 정의하고 관련 메타 정보를 저장한다. 클라이언트는 서버와 인공지능 모델 혹은 에이전트 사이에서 도구 호출과 정보 전달을 중계한다. MCP는 시스템 독립적이며, 다양한 기능과 인터페이스를 가진 도구를 표준화된 방식으로 통합하여 활용할 수 있는 장점이 있다.

본 논문에서 제안하는 MCP 기반 도구 연동 플랫폼은 기존 기술과 다음과 같은 차별점이 있다.

(1) 사이버범죄 수사 추론 에이전트에서 분석·추론 도구의 통합 및 활용을 위한 동적 연결 및 기능 등록을 지원

(2) 사이버범죄 수사 추론 에이전트가 복합적 사건에 대응할 수 있도록 표준화된 도구 호출 및 연동 메커니즘을 제공

Ⅲ. MCP 기반 도구 연동 플랫폼

제안하는 플랫폼의 구조는 그림 1과 같다. 이 플랫폼은 다중 MCP 서버 지원, MCP 서버 관리, 도구 연결 및 기능 등록, 그리고 MCP 프록시로 구성된다. 연동 도구는 런타임 중에 동적으로 연결 및 해제할 수 있다. MCP 프록시는 API 파라미터, 도구 기능 목록, MCP 서버 연결 주소 등 필수적인 연동 정보를 관리한다.

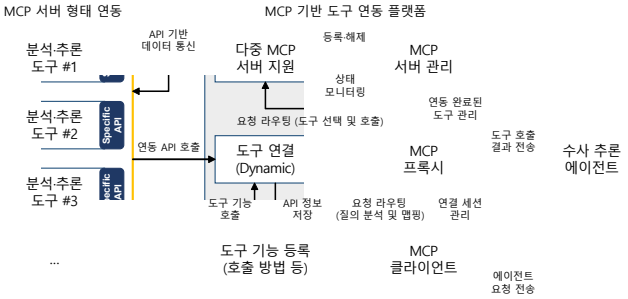

그림 1. MCP 기반 도구 연동 플랫폼 구조

개별 분석·추론 도구는 도구 연결 및 기능 등록 API를 사용하여 MCP 서버 형태로 플랫폼에 연동할 수 있다. 해당 API의 명칭 및 사용 방법은 표 1과 같다.

API 명칭	사용 방법 예시

도구 동적 연결	[POST]
	{base_url}/tool_dynamic_integration
	[필요 파라미터 목록]
	{
	"name":"human_network_analysis",
	"url":"http://123.456.789:8000",
	"timeout":30
	}

도구 기능 등록 (API 명세 정보)	[POST]
	{base_url}/tool_api_registration/{tool_name}/endpoints
	[필요 파라미터 목록]
	{
	"endpoints":[
	{
	"method":"GET",
	"path":"/users",
	"description":"Get information of all users"
	},
	...
	]
	}

도구 기능 호출	[POST]
	{base_url}/tool_api_registration/{tool_name}/call
	[필요 파라미터 목록]
	{
	"method":"GET",
	"path":"/users",
	"params":{}
	}

표 1. 도구 연결 및 기능 등록 API

MCP 프록시는 연결 및 기능 등록이 완료된 도구를 관리하며, 수사 추론 에이전트의 요청 정보를 수신한다. 에이전트로부터 라우팅되는 요청 정보는 직접 질의 혹은 핵심 키워드 형태로 정의된다. 예를 들어, "네트워크 분석"이라는 키워드가 전달되었을 경우 MCP 프록시는 등록 완료된 도구 목록을 조회하고, 키워드 매칭 혹은 기능 태그 분석을 통해 해당 기능을 보유한 도구를 탐색한다. 탐색의 결과로 도구 선택이 완료되면, 도구의 API 정보를 활용하여 필요한 기능을 호출한 다음 결과를 수신하여 에이전트로 반환한다. MCP 기반 도구 연동 플랫폼은 현재 연결 중인 도구의 상태를 주기적으로 모니터링한다. 또한, 도구 개발자를 위해 연동 규격 및 API 명세를 상세 사용 가이드 형태로 제공한다.

그림 2. MCP 기반 도구 연동 플랫폼 테스트(도구 연결 후 기능 등록)

제안하는 플랫폼을 검증하기 위해 플랫폼 세부 기능을 구현하고 테스트 환경을 구축하였다. 그림 2는 도구 연결 후 기능 동록에 대한 테스트 결과를 보여준다. 플랫폼 테스트에는 임의 구현된 네트워크 분석 도구를 활용하였다. MCP 기반 도구 연동 플랫폼은 동적 연결, 기능 등록 및 호출에 관한 절차를 API 형태로 관리함으로써 사용자가 적시적소에 수사 추론 에이전트에 필요한 도구를 연동할 수 있다. 도구 연결에 소요되는 시간은 1초 이내로 사용자 체감이 적은 수준이었으며, 이미 연결이 완료된 도구의 기능 호출은 플랫폼에서 큰 부하 없이 처리하는 것을 확인하였다.

Ⅳ. 결론 및 향후 연구

본 논문에서는 사이버범죄 수사 추론 에이전트를 위한 MCP 기반 도구 연동 플랫폼을 제안하였다. 제안된 플랫폼은 다양한 분석·추론 도구와의 표준화된 연동 인터페이스를 제공함으로써 수사 추론 에이전트가 상황에 맞는 도구를 선택 및 실행할 수 있도록 지원한다. 이를 통해 사이버범죄 사건에 대한 통합적인 분석과 수사 지원에 기여할 수 있다.

향후 연구로는 사이버범죄 수사 추론 시나리오를 구성하여 MCP 기반 도구 연동 플랫폼을 테스트하고 세부 기능을 개선하는 것이 있다. 또한, 다수의 도구에 대한 연결 및 기능 등록의 응답시간 및 처리량 측정 실험을 수행하여 플랫폼 운용 성능을 최적화할 계획이다.

ACKNOWLEDGMENT

이 논문은 2025년도 행정안전부의 재원으로 과학치안진흥센터 사이버범죄 수사단서 통합분석 및 추론시스템 개발 사업의 지원을 받아 수행된 연구임(No. RS-2025-02218280)

참 고 문 헌

[1] 이연주, 이서연, 김기범, 이성진, "사이버범죄 발생과 공간의 연관성 분석 - 공간회귀분석을 활용하여 서울특별시를 중심으로", 디지털 포렌식 연구, vol. 17. no. 4, pp. 128-145, Dec. 2023.

[2] H. Kim, D. Kim, J. Lee, C. Yoon, D. Choi, M. Gim, and J. Kang, "LAPIS: Language Model-Augmented Police Investigation System", Proc. of the ACM International Conference on Information and Knowledge Management, pp. 4637-4644, Oct. 2024.

[3] 이소현, 강일웅, 정윤혁, 김희웅, "사이버범죄 유형별 특징 분석 연구", Information Systems Review, vol. 21, no. 3, pp. 1-26, Jan. 2019.

[4] S. Liu, H. Miao, and P-T. Bremer, "ParaView-MCP: An Autonomous Visualizatiion Agent with Direct Tool Use", arXiv preprint arXiv:2505.07064, pp. 1-6, May 2025.