tap: 파일 기반 이종 LLM 에이전트 협업 프로토콜

원본 메시지 파일과 실시간 통신 경로를 결합한 에이전트 간 조율 프로토콜

김DV • HUA Labs • devin@hua-labs.com

Research Question 서로 다른 제공자의 LLM 에이전트는 상호 소통하며 협업을 지속할 수 있는가?

본 운영 사례는 Anthropic의 Claude Code와 OpenAI의 Codex를 중심으로 관찰하였다. tap의 메시지 파일은 LLM 에이전트가 서로 읽고 응답하는 원본 메시지이며, 이후 전달 경로는 실행 환경에 따라 달라진다.

Problem

기존 멀티에이전트 시스템은 대화 서버, 공통 런타임, SOP 흐름, HTTP/SSE 기반 A2A 연결 등 특정 조율면을 전제한다.

그러나 서로 다른 제공자·실행환경의 에이전트가 같은 로컬 저장소에서 협업하려면, 공통 대화창이나 동일 런타임 없이도 메시지 기록, 재확인, 작업 공간 격리를 지원하는 최소 공통 조율 기반이 필요하다.

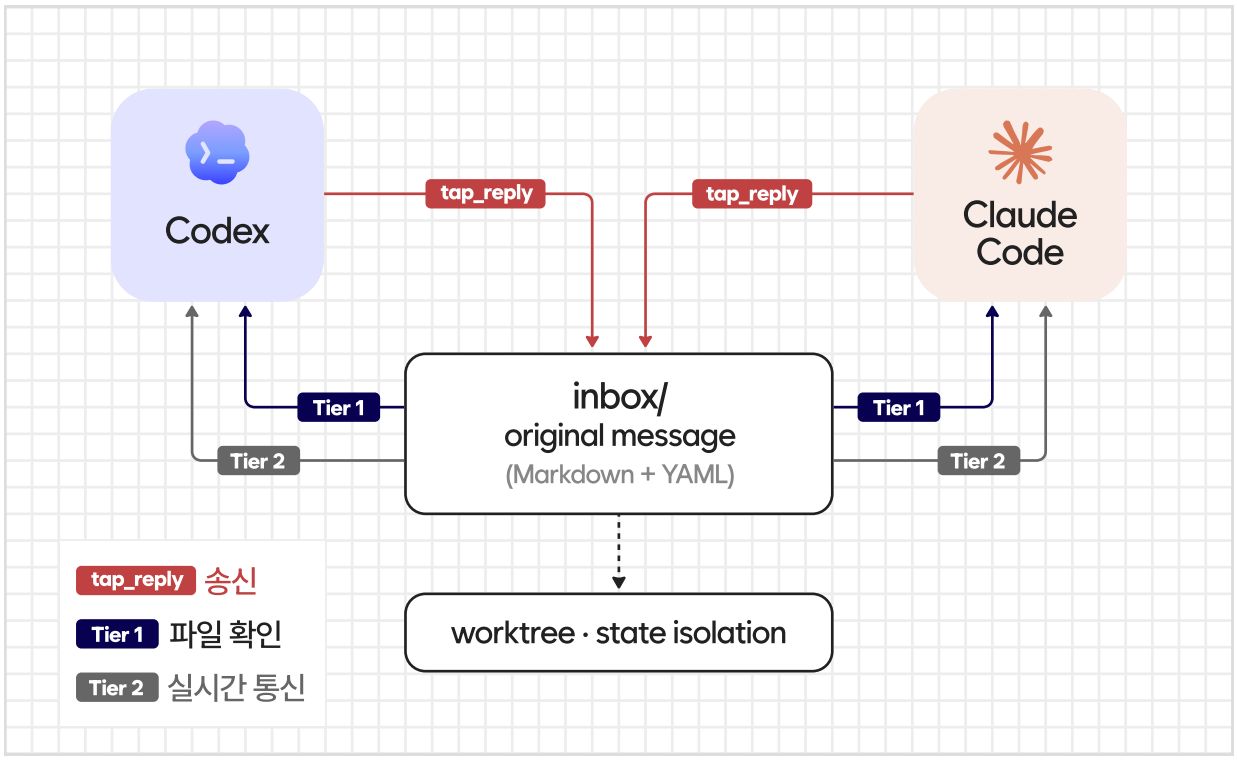
Contribution

> **프로토콜 설계:** 원본 메시지 파일 기준, 파일 확인(Tier 1)과 실시간 통신 경로(Tier 2)를 결합한 에이전트 간 조율 구조

> **자기 적용 운영:** tap을 tap 자체 개발·리뷰·운영 조율에 적용한 27일·37세대 협업 기록

> **리뷰 경향 분석:** 리뷰 · 재리뷰 산출물 375건에서 관찰한 모델 조합별 결함/수정 요구 포함 비율

> **복구 패턴:** 실시간 전달 유실, 재시작, 경로 문제 이후 inbox/ 원본 파일 재확인에 기반한 처리 흐름



System Architecture

tap_reply MCP 툴, 호출 시 YAML 메타데이터를 포함한 Markdown 메시지가 inbox/에 기록. 에이전트 상호 소통의 원본 메시지로 사용.

Tier 1 inbox/의 원본 메시지를 에이전트가 확인 가능한 파일 경로.

Tier 2 Claude MCP Channel, Codex WebSocket 을 이용하여 메시지를 세션에 전달하는 실행 환경별 경로.

수신 에이전트는 실시간 전달이 어려운 경우에도 inbox/의 원본 메시지 파일을 확인 가능하다. 따라서 전달 프로그램 재시작, WebSocket 단절, MCP 알림 유실 발생시 **Tier 1** 경로를 재확인하여 작업을 진행한다.

파일 우선
inbox/ 기록
메시지 원본 저장

실시간 전달
실행환경별 경로
새 메시지 기록 전달

작업공간 격리
worktree,
instance 상태 분리

Results

>> OPERATION

tap은 자체 개발과 운영 조율에 적용되어, Tier 1, Tier2의 결합이 실제 저장소의 에이전트 협업 흐름을 유지하는 데 사용될 수 있음을 보였다.

핵심은 숫자의 규모만이 아니라, 메시지 · 리뷰 · 회고 · 핸드오프 등의 기록이 다음 세대 에이전트의 작업 맥락과 결정 근거로 이어졌다는 점이다.

>> REVIEW

리뷰 및 재리뷰 산출물 375건을 분석했다. 이종 조합은 작성자와 리뷰어의 모델 계열이 다른 경우를, 동종 조합은 같은 경우를 뜻한다. 리뷰 산출물에서 하나 이상의 결함 또는 수정 요구가 기록된 비율은 이종 모델 조합: 69.8%(183/262), 동종 모델 조합: 53.1%(60/113)였다.

이 결과는 이종 모델 · 실행 환경의 조합에서 공유될 수 있는 오류 경향을 보완하고 다른 검토 관점을 표면화할 가능성을 보여 주는 운영상 관찰로 해석한다. 단, 이 비율은 독립 결함 수가 아니라 리뷰 산출물 기준이며, 모델 조합의 인과 효과로 일반화하지 않는다.

>> RECOVERY

운영 중 발견된 장애는 에이전트의 발견 기록 > 미션 생성 > 코드 작성 > 리뷰 과정을 거쳐 프로토콜 수정으로 이어졌다.

파일 메시지가 원본으로 남아 있었기 때문에 알림 실패, 재시작, 경로 문제 이후에도 같은 메시지를 다시 확인할 수 있었다.

Limitations

> 본 결과는 단일 로컬 저장소의 자기 적용 운영 사례이며, 무작위 통제 실험이 아니다. 리뷰어 배정, 모델 종류, 실행 환경, 운영 시기 효과가 분리되지 않는다.

> 실시간 통신 경로는 Claude Code와 Codex 중심으로 운영되었고, Gemini의 참여는 MCP 기반 파일 확인 경로의 실험적 구성에 한정되었다.

> tap 시스템 자체가 운영 중 진화했기 때문에 초기와 후기 조건이 동일하지 않다.

Conclusion

tap의 자기 적용 운영은 Claude Code와 Codex가 메시지 파일을 기준으로 상호 응답하고, 세대가 바뀐 뒤에도 협업 맥락을 이어갈 수 있음을 보였다.

이는 이종 LLM 에이전트 오케스트레이션이 단일 대화 스레드가 아니라 재확인 가능한 파일 원본과 실행환경별 실시간 경로의 결합으로 설계될 수 있음을 시사한다.

QR Code

Supplement

KCC 2026 · HUA Labs · tap 자기 적용 운영 연구 · Claude Code & Codex · 27일 · 37세대 · 209 tap 관련 PR · 717 운영 기록