Contribution ID: **139** Type: **Poster Presentation**

A Dynamic LLM-Based Multi-Agent Collaboration for Network Security Operations

Abstract

With the continuous expansion of large scientific facilities and critical research infrastructures, the network security operations of their network systems face growing challenges such as massive data volumes, high alarm complexity, and low efficiency of manual processing. Traditional security operations methods rely heavily on human analysis and experience, which are inadequate for coping with dynamic and complex security threats. To enhance the level of network security protection and operational intelligence, this paper proposes an intelligent network security framework that integrates Large Language Models (LLMs) with a multi-agent collaboration mechanism. The goal is to build a new intelligent network security operation architecture capable of autonomous decision-making, collaborative reasoning, and closed-loop task execution.

In this study, the LLM serves as the intelligent core, around which a multi-agent collaborative architecture tailored to network security operations scenarios is designed. Each functional agent, based on a unified security knowledge base and contextual information, is responsible for tasks such as knowledge retrieval, database operations, command generation, logical reasoning, and report writing. This enables intelligent collaboration across the entire process—from threat detection to response handling. To support information sharing and task decomposition among agents, the system integrates key technologies such as Retrieval-Augmented Generation (RAG), Text-to-SQL, Text-to-Command, and Chain-of-Thought (CoT) reasoning. These enhance the agents' abilities in knowledge augmentation, logical reasoning, and tool utilization, thereby improving comprehension and execution in complex security operations tasks. Through a unified context interaction interface and scheduling mechanism, the system achieves coordinated orchestration and result aggregation among agents, forming an intelligent closed loop for security event analysis, response, and report generation.

During experimental validation, suitable models were fine-tuned on network security datasets to optimize the accuracy of Text-to-SQL task execution. The effectiveness of the multi-agent collaboration mechanism was further verified in tasks such as alert analysis, event correlation, and automated report generation. The results demonstrate that the proposed hybrid architecture significantly improves the accuracy and efficiency of security event analysis and response, realizing a shift from "human-assisted" to "intelligent collaborative" network security operations.

This research provides a scalable technical pathway for intelligent network securityoperations, offering theoretical and practical references for building autonomous, trustworthy, and interpretable intelligent operations systems. It also lays the groundwork for the deep integration and application of LLMs and multi-agent systems in the field of cybersecurity.

Keywords: Large Language Model; Multi-Agent Collaboration; Network Security; Intelligent Operations and Maintenance; Retrieval-Augmented Generation.

Primary authors: [illegible]; [illegible]; [illegible]; [illegible]

Presenter: [illegible]

Track Classification: Track 7: Network, Security, Infrastructure & Operations