arXiv:2507.21653v1 [cs.LG] 29 Jul 2025

DGP: A Dual-Granularity Prompting Framework for Fraud Detection with Graph-Enhanced LLMs

Yuan Li[1], **Jun Hu**[1], **Bryan Hooi**[1], **Bingsheng He**[1], **Cheng Chen**[2]

[1]National University of Singapore [2]ByteDance Inc.

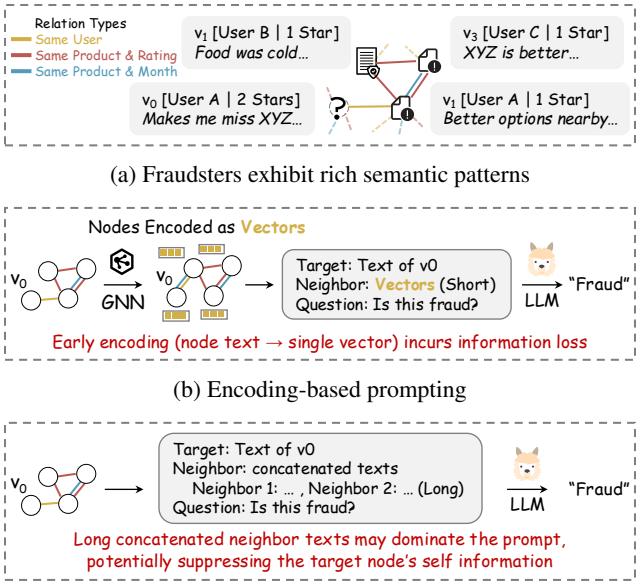
li.yuan@u.nus.edu, {jun.hu, dcsbhk, dcsheb}@nus.edu.sg, chencheng.sg@bytedance.com

Abstract

Real-world fraud detection applications benefits from graph learning techniques that jointly exploit node features—often rich in textual data—and graph structural information. Recently, Graph-Enhanced LLMs emerge as a promising graph learning approach that converts graph information into prompts, exploiting LLMs' ability to reason over both textual and structural information. Among them, text-only prompting, which converts graph information to prompts consisting solely of text tokens, offers a solution that relies only on LLM tuning without requiring additional graph-specific encoders. However, text-only prompting struggles on heterogeneous fraud-detection graphs: multi-hop relations expand exponentially with each additional hop, leading to rapidly growing neighborhoods associated with dense textual information. These neighborhoods may overwhelm the model with long, irrelevant content in the prompt and suppress key signals from the target node, thereby degrading performance. To address this challenge, we propose Dual Granularity Prompting (DGP), which mitigates information overload by preserving fine-grained textual details for the target node while summarizing neighbor information into coarse-grained text prompts. DGP introduces tailored summarization strategies for different data modalities—bi-level semantic abstraction for textual fields and statistical aggregation for numerical features—enabling effective compression of verbose neighbor content into concise, informative prompts. Experiments across public and industrial datasets demonstrate that DGP operates within a manageable token budget while improving fraud detection performance by up to 6.8% (AUPRC) over state-of-the-art methods, showing the potential of Graph-Enhanced LLMs for fraud detection.

1 Introduction

Graph-based fraud detection has emerged as a critical research direction, driven by its effectiveness in capturing the complex relational patterns inherent in real-world data (Xu et al. 2024; Akoglu, Tong, and Koutra 2015; Rayana and Akoglu 2015; McAuley and Leskovec 2013) benefit from advanced graph learning techniques.



(a) Fraudsters exhibit rich semantic patterns

(b) Encoding-based prompting

(c) Text-only prompting

Figure 1: Graph-to-prompt methods for fraud detection.

Graph-Enhanced LLMs for Fraud Detection. In recent years, various Graph Neural Networks (GNNs) have been proposed for graph-based fraud detection, achieving notable success by leveraging neighborhood information and structural patterns to enhance detection accuracy (Duan et al. 2024; Li et al. 2024). More recently, graph-enhanced Large Language Models (LLMs) have emerged as a promising alternative for graph-based fraud detection tasks, leveraging their generalizable language capabilities and demonstrating competitive performance across a range of tasks (Tang et al. 2024a,b; Liu et al. 2024b). These approaches have shown potential in analyzing the rich semantics associated with fraudulent nodes, as well as the diverse relationships among them (as illustrated in Figure 1a), by exploiting the semantic nuances within the graph (Tang et al. 2024a). Notably, we distinguish these methods from LLM-enhanced GNNs such as TAPE (He et al. 2024) and FLAG (Yang et al. 2025),

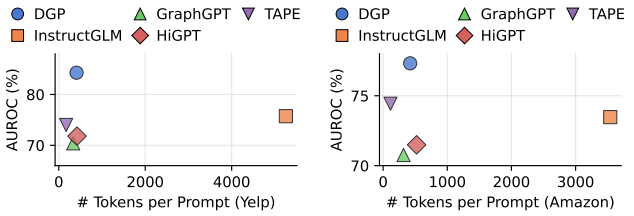


Figure 2: Fraud detection performance (↑) *vs*. token usage per prompt (↓) across different methods and datasets. Our proposed method, DGP, achieves top performance with moderate token consumption, demonstrating a notable balance between token usage and performance.

which incorporate LLM-encoded features and rely heavily on the classification capabilities of GNNs. In this work, we focus on leveraging graph-enhanced LLMs as standalone classifiers to fully explore their potential in graph-based fraud detection.

To bridge the gap between graph-structured data and LLMs, graph-enhanced LLMs transform graph data into textual prompts (graph-to-prompt) to naturally integrate both graph structure and semantics into LLMs (Fatemi, Halcrow, and Perozzi 2023; Ye et al. 2024). Two major graph-to-prompt strategies, as depicted in Figure 1b and 1c, have been developed in recent literature: (1) Encoding-based prompting, exemplified by approaches such as GraphGPT (Tang et al. 2024a) and HiGPT (Tang et al. 2024b), encodes nodes into compact vectors and subsequently feeds them into an LLM. These methods substantially reduce prompt length via node encoding, but suffer from early vectorization, leading to **information loss** due to reduced semantic-level interactions (Li et al. 2023). In contrast, (2) text-only prompting (Wang et al. 2023; Ye et al. 2024; Fatemi, Halcrow, and Perozzi 2023; Zhu et al. 2025) preserves detailed semantic interactions by concatenating neighbor texts into the prompt. However, these methods inherently suffer from excessive prompt length, leading to **distraction from crucial content** due to information overload. For example, in industrial scenarios, each neighboring node can be associated with over 1,500 tokens, resulting in a 2-hop neighborhood with up to 2 million tokens, which poses challenges for incorporating dense textual information for fraud detection.

In this work, we propose **D**ual **G**ranularity **P**rompting (DGP), a novel text-only prompting framework that leverages the rich semantics on graphs while addressing the challenge of excessive prompt length. To reduce the information loss incurred by early-stage encoding, DGP selectively preserves fine-grained text for the target node while summarizing neighbors retrieved from different metapaths into compact, coarse-grained texts. For textual features, we employ bi-level semantic summarization to reduce the prompt length. For numerical features, we adopt precise numerical summarization to retain key insights. As illustrated in Figure 2, our approach achieves an impressive balance between token usage and performance. Compared to prior state-of-the-art methods, DGP operates with a manageable prompt length while improving fraud detection performance by up to 6.8% (AUPRC), demonstrating the effectiveness of our dual-granularity design with reasonable token budgets.

The key contribution of this work is three-fold:

- We propose DGP, a novel graph prompting framework that integrates fine-grained textual details for target nodes with coarse-grained semantic summaries for their neighbors, thereby overcoming limitations faced by existing graph-to-prompt methods.
- We introduce specialized summarization strategies for compressing neighborhoods associated with textual and numerical features into concise, semantically meaningful prompts tailored for LLM processing.
- Extensive experiments on public and industry datasets demonstrate the superior empirical performance of DGP, achieving manageable prompt lengths while improving fraud detection performance by up to 6.8% in AUPRC compared to state-of-the-art approaches.

2 Related Work

2.1 Graph Neural Networks for Fraud Detection

Graph neural networks (GNNs) have become the dominant approach for fraud detection by modeling relational patterns in graphs (Akoglu, Tong, and Koutra 2015; Rayana and Akoglu 2015; Duan et al. 2024; Li et al. 2024). Classic models such as GCN (Kipf and Welling 2017) and GAT (Veličković et al. 2018) have inspired many variants targeting specific challenges, including camouflage (CARE-GNN (Dou et al. 2020)), heterophily (PMP (Zhuo et al. 2024)), and limited supervision (ConsisGAD (Chen et al. 2024), barely-supervised learning (Yu, Liu, and Luo 2024)). However, most GNN-based approaches underutilize the fine-grained textual semantics widely available in real-world graphs, which our method explicitly addresses.

2.2 Integrating LLMs with Graphs

Recent advances in integrating LLMs with graph data can be broadly classified into *graph-enhanced LLMs* and *LLM-enhanced GNNs*. Graph-enhanced LLMs primarily adopt graph-to-prompt strategies, which can be divided into encoding-based prompting and text-only prompting. Encoding-based prompting (Tang et al. 2024a,b) compresses graph features for LLM input, potentially resulting in semantic loss. Specifically, GraphGPT (Tang et al. 2024a) aligns LLMs with graph structural information via a dual-stage instruction-tuning paradigm and a graph-text alignment projector. HiGPT (Tang et al. 2024b) extends instruction tuning to heterogeneous graphs by introducing an in-context heterogeneous-graph tokenizer and heterogeneity-aware fine-tuning. In contrast, text-only prompting (Fatemi, Halcrow, and Perozzi 2023; Ye et al. 2024; Zhu et al. 2025) concatenates the texts of neighboring nodes as input to LLMs, which may lead to excessively long prompts and distract from crucial information. For example, InstructGLM (Ye et al. 2024) frames graph tasks as natural-language instructions for generative LLMs, enabling node classification on citation networks.