시계열 특성을 활용한 다양한 이상 거래 탐지 딥러닝 모델 개발과 성능 분석

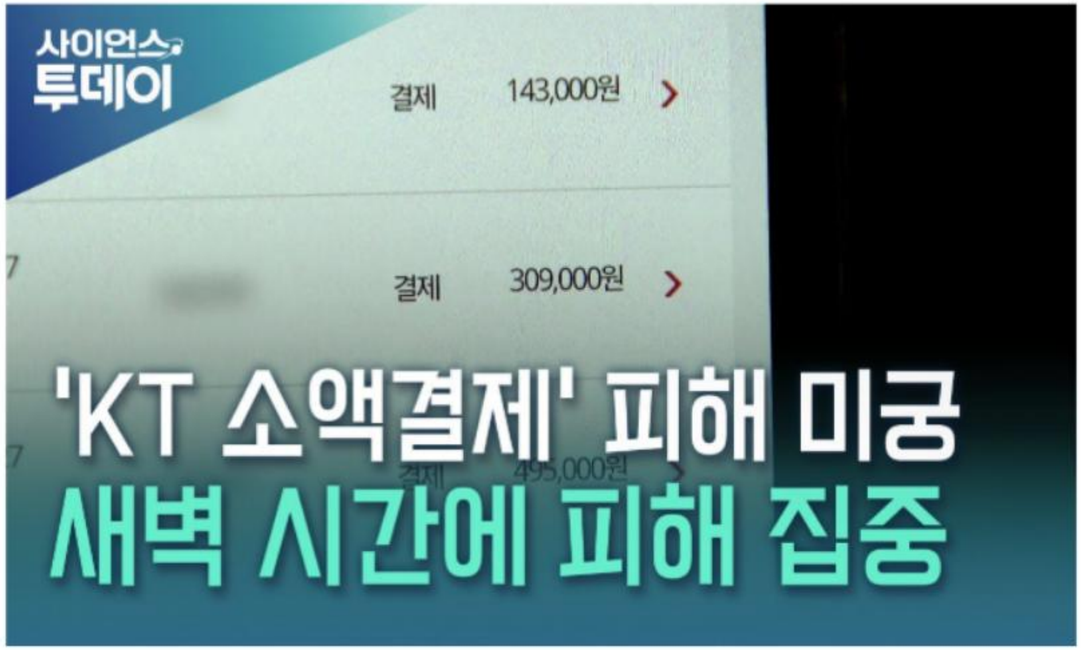
Team04
팀명: 송골매
지도교수: 송길태
팀원: 배근호, 추민, 윤소현

2025.09.26

목 차

시계열 특성을 활용한 다양한 이상 거래 탐지
딥러닝 모델 개발과 성능 분석

연구 배경



2025년 9월 9일, 출처: https://youtu.be/RfZSZnX-KwU

KT·롯데카드 연이은 해킹 피해 ...정부 '근본 대책 마련'

류제명 과학기술정보통신부 제2차관과 권대영 금융위원회 부위원장이 19일 오전 서울 종로구 정부서울청사에서 열린 해킹 대응을 위한 과학기술정보통신부-금융위원회 합동 브리핑에서 KT 및 롯데카드 해킹 사태 질문에 답하고 있다

2025년 9월 19일, 출처:
https://www.bbc.com/korean/articles/cqxzg08dl01o

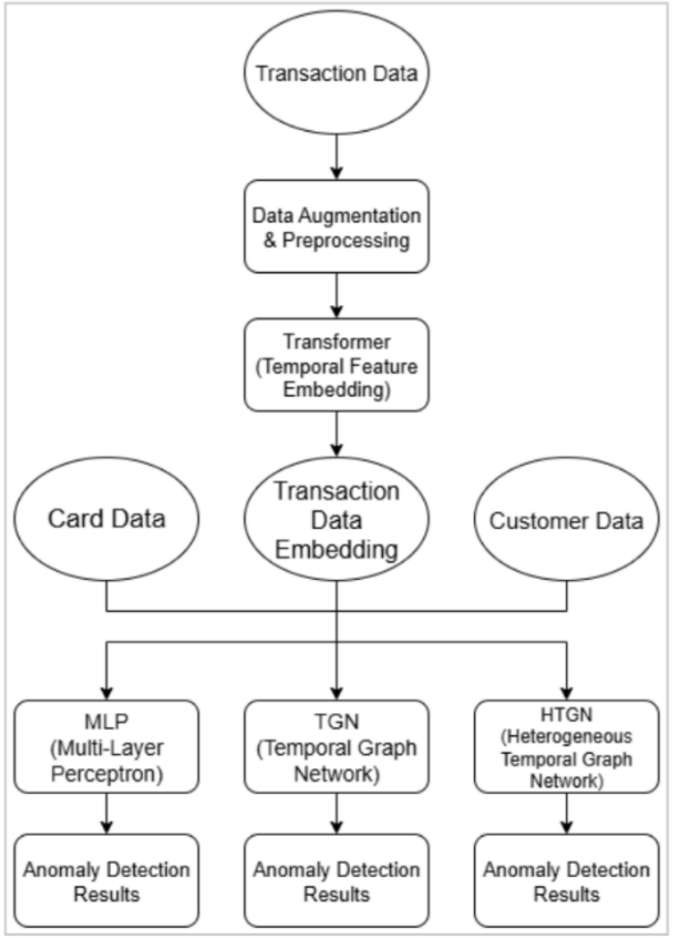
시계열 특성을 활용한 다양한 이상 거래 탐지 딥러닝 모델 개발과 성능 분석

기존 탐지 시스템 한계 및 거래 시계열

date	card_id	amount	merchant_id	merchant_city	merchant_state	zip	mcc	fraud
2016-05-09 22:18	3159	$100.00	27092	Clearfield	KY	40313	4829	0
2016-05-10 6:02	3159	$3.32	75936	Louisville	KY	40299	5814	0
2016-05-10 12:35	3159	$406.84	7472	New Albany	IN	47151	5300	1
2016-05-10 13:22	3159	$57.60	41184	ONLINE	ONLINE	00000	5310	1
2016-05-10 14:01	3159	$168.56	68192	Laconia	IN	47135	5310	1
2016-05-10 14:02	3159	$42.67	27092	ONLINE	ONLINE	00000	4829	1
2016-05-10 17:35	3159	$120.27	60569	ONLINE	ONLINE	00000	5300	1
2016-05-10 20:36	3159	$54.00	56431	Louisville	KY	40299	5541	0
2016-05-11 6:22	2682	$3.37	75781	Georgetown	KY	40324	5411	0
2016-05-12 0:32	2682	$23.95	75781	Georgetown	KY	40324	5411	0
2016-05-12 5:42	3159	$16.32	33120	Louisville	KY	40299	5813	0
2016-05-13 5:40	3159	$15.01	33120	Louisville	KY	40299	5813	0

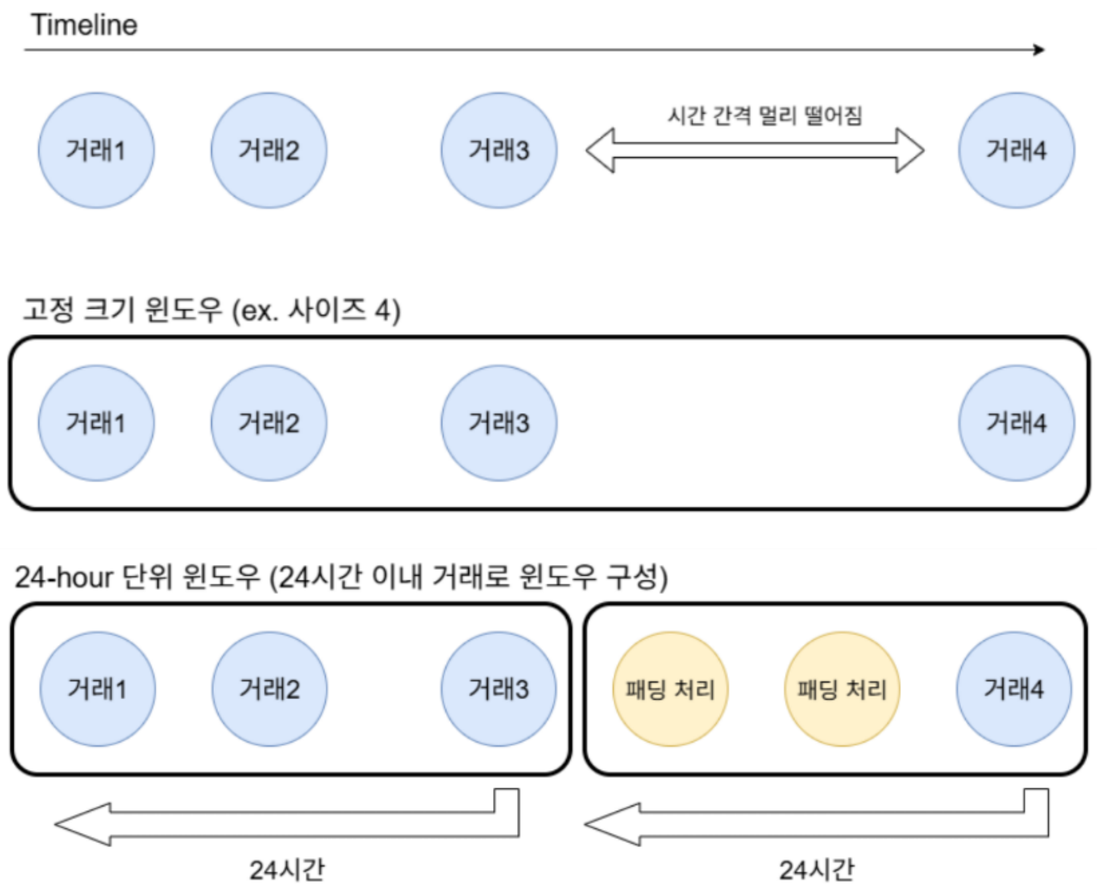
시계열 특성을 활용한 다양한 이상 거래 탐지
딥러닝 모델 개발과 성능 분석

데이터 흐름도



시계열 특성을 활용한 다양한 이상 거래 탐지 딥러닝 모델 개발과 성능 분석

트랜스포머 임베딩: 거래 시계열 맥락 반영

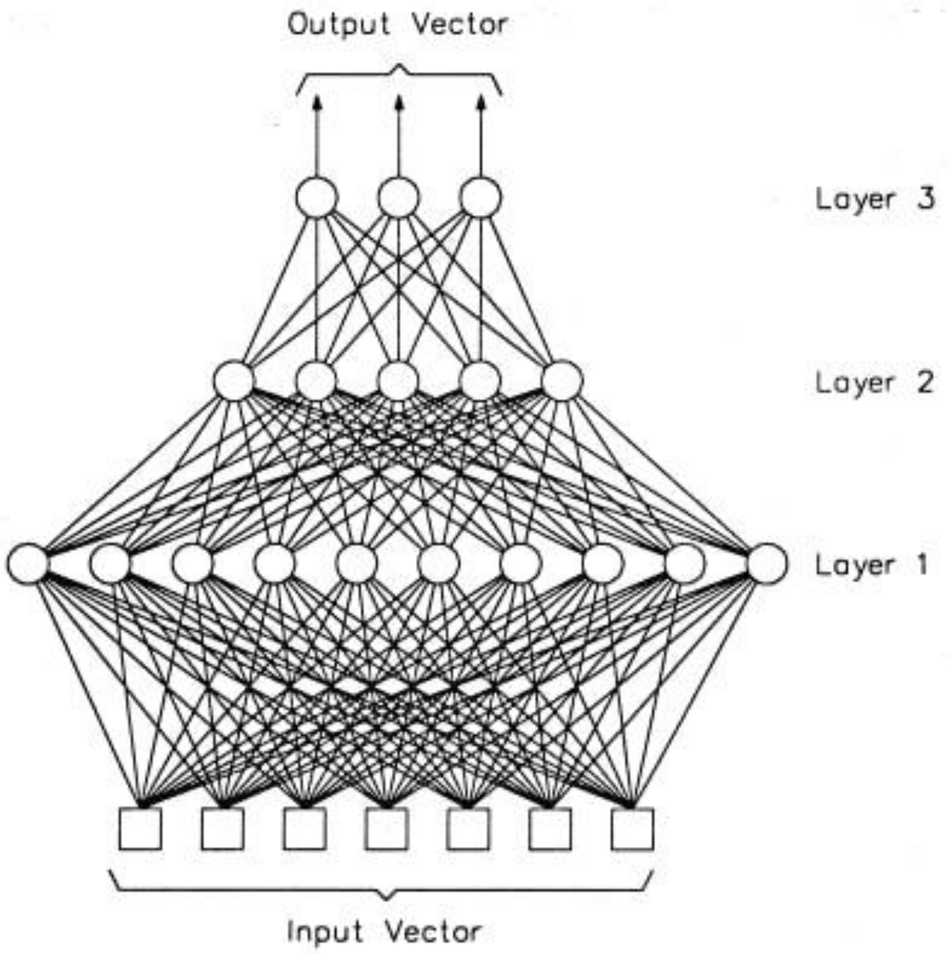


- 과거 거래와 현재 거래의 시간적 연관성을 임베딩으로 추출

- 윈도우 구성을 24시간 단위로 변경
→ 짧은 시간 내 반복되는 이상 거래 반영 가능

시계열 특성을 활용한 다양한 이상 거래 탐지
딥러닝 모델 개발과 성능 분석

MLP란?



출처:https://deepestdocs.readthedocs.io/en/latest/004_deep_learning_part_2/0040/

- 퍼셉트론으로 이루어진 층(layer) 여러 개를 순차적으로 붙여놓은 형태

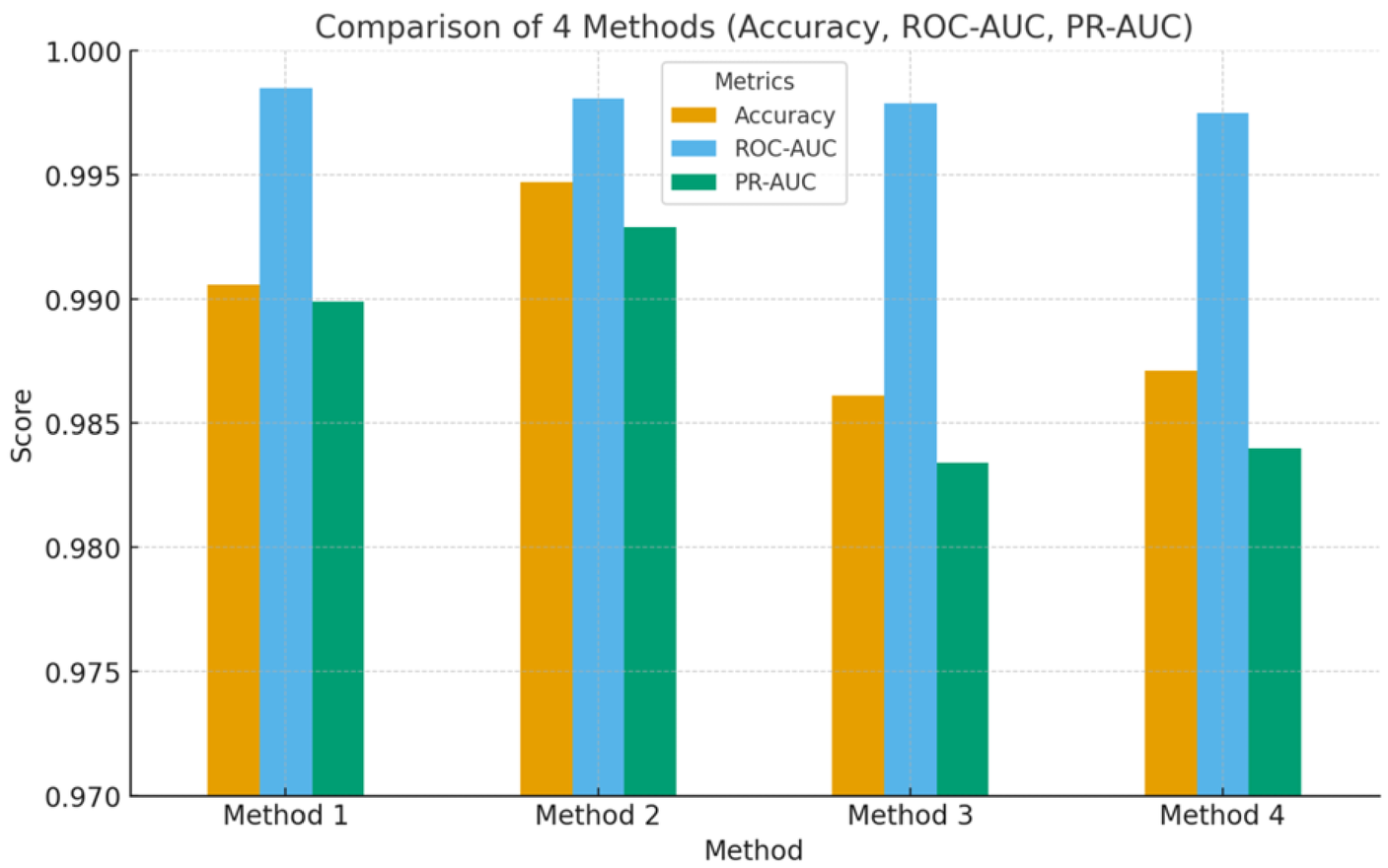
- 각 층은 그래프 구조에서 하나의 노드처럼 동작함

MLP 아이디어

4가지 관점의 모델링 아이디어

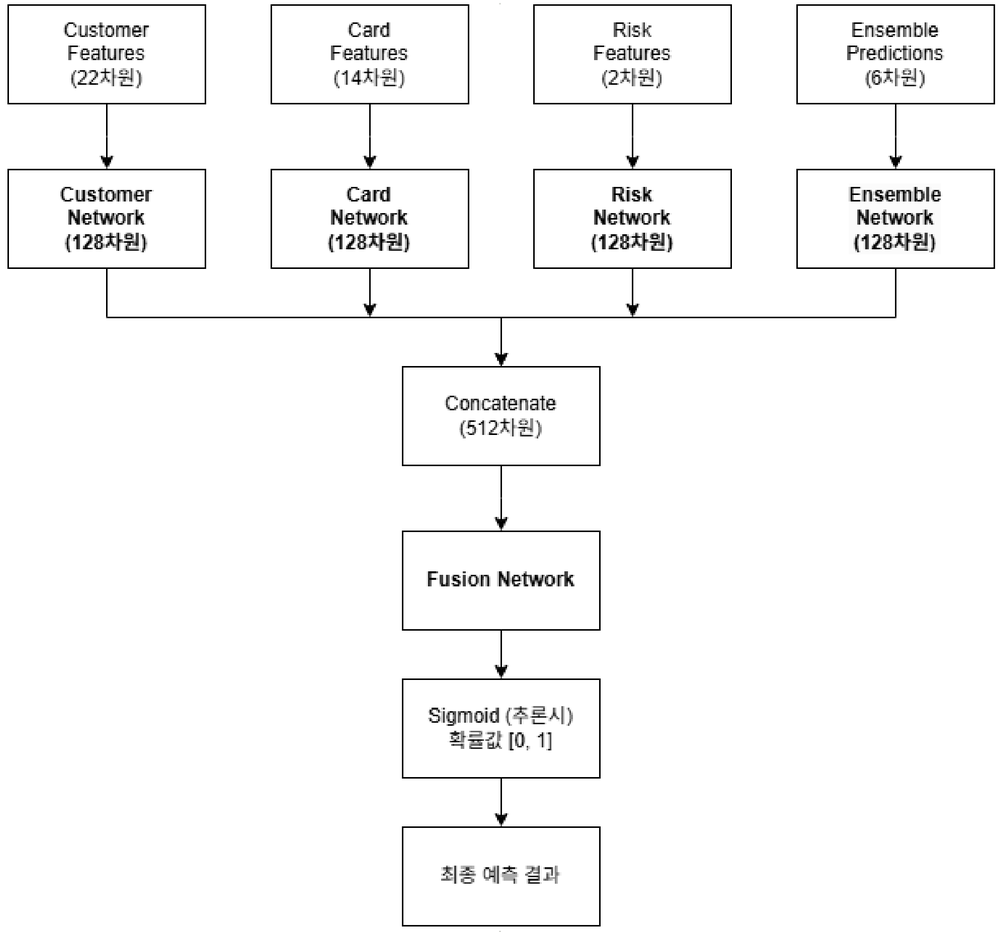
- **Method 1 (임베딩 + 집계)**: 거래 임베딩과 고객/카드 요약 통계를 결합하여 **개별 거래의 맥락과 장기적 특성**을 함께 학습합니다.
- **Method 2 (윈도우 평탄화)**: 시간 순서에 따른 거래 패턴을 MLP가 직접 학습하도록 **시계열적 연속성**을 모델링합니다.
- **Method 4 (이상 패턴 감지)**: Z-score, IQR 등 통계 지표를 활용해 개인의 **정상 거래 패턴에서 벗어나는 미묘한 변화**를 포착합니다.
- **Method 3 (시간 구간 분할)**: 거래 데이터를 고정된 시간 단위(예: 1시간, 24시간)로 나누고, 각 구간별 통계 특징을 집계하여 패턴을 분석합니다.

MLP 아이디어 성능 비교



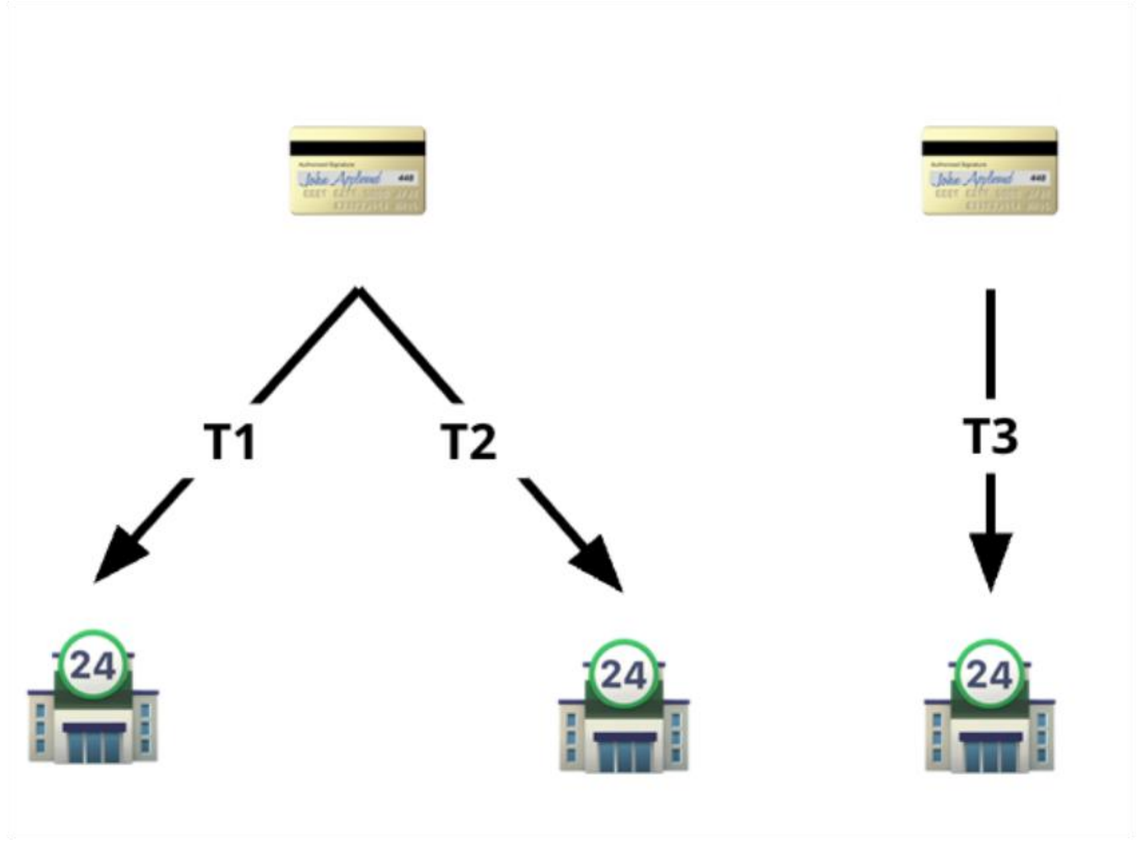
시계열 특성을 활용한 다양한 이상 거래 탐지
딥러닝 모델 개발과 성능 분석

최종 MLP 모델 구조



시계열 특성을 활용한 다양한 이상 거래 탐지 딥러닝 모델 개발과 성능 분석

Temporal Graph Network (TGN) 란?



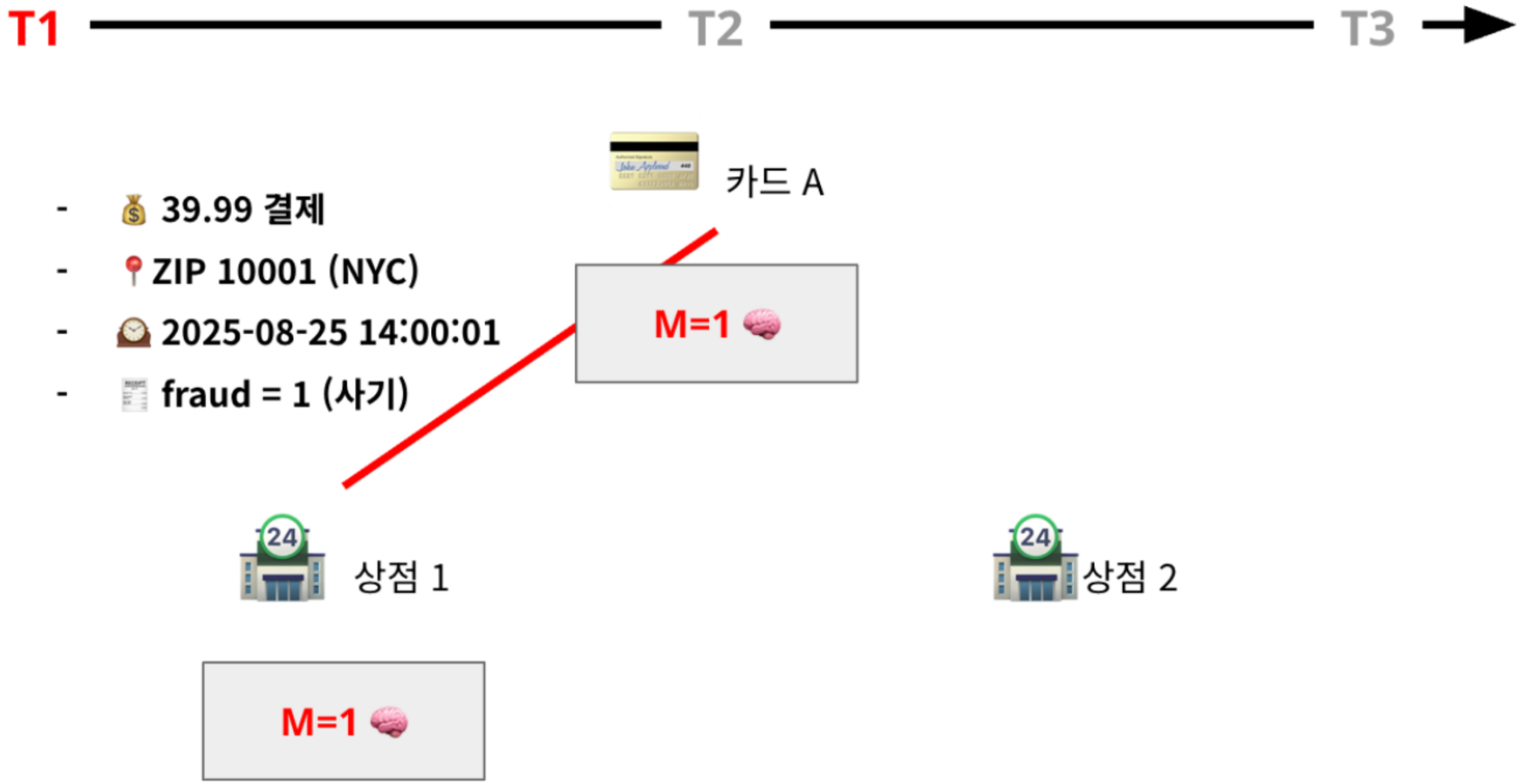
- 시간 순서대로 발생하는 거래 이벤트 처리
- 카드/상점 노드가 개별 메모리를 가짐
- 거래 발생 시 연결된 두 노드의 메모리 동시 업데이트
- 과거 맥락을 반영하여 사기 여부를 예측

시계열 특성을 활용한 다양한 이상 거래 탐지
딥러닝 모델 개발과 성능 분석

TGN의 시간순 거래 처리 (1)

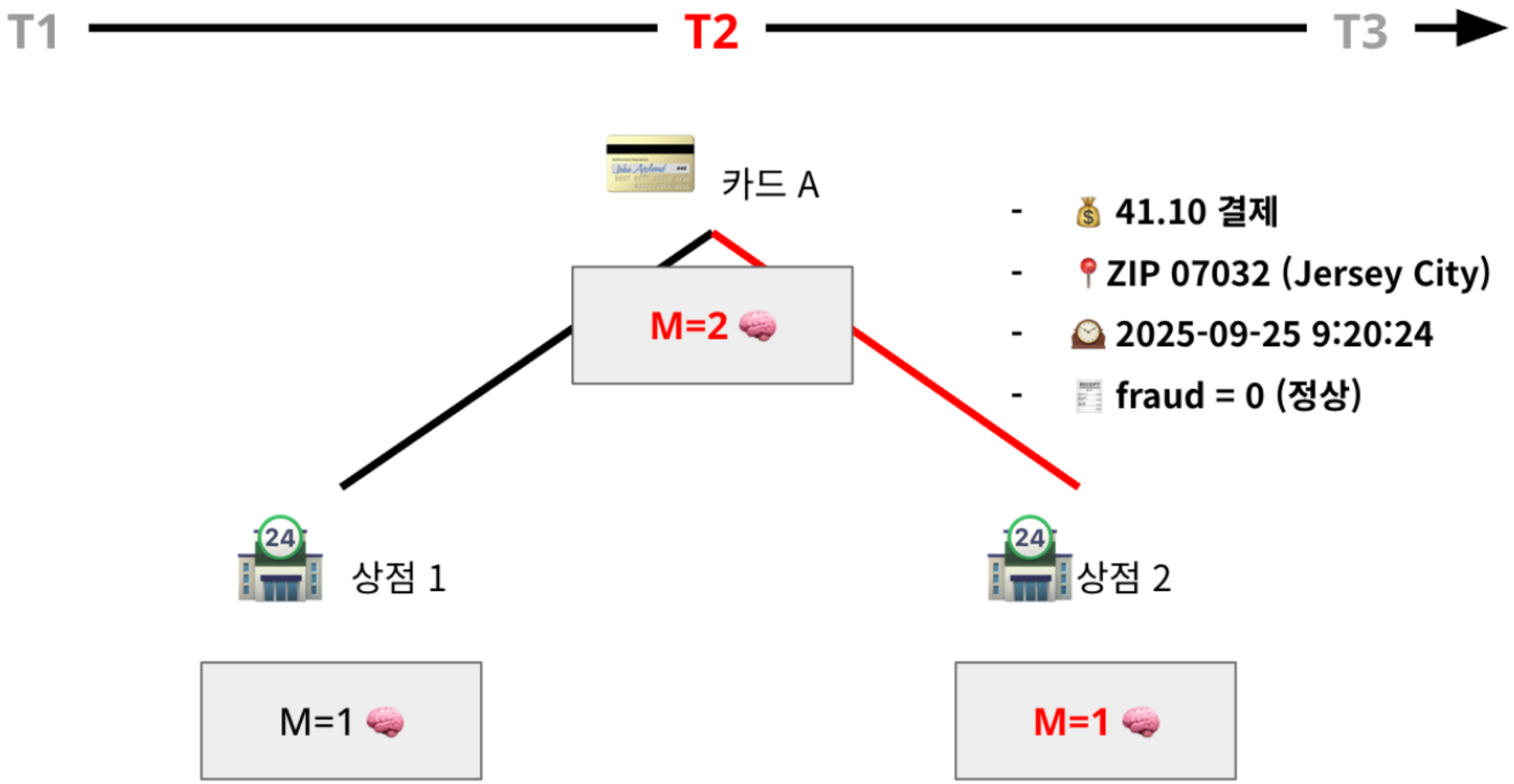
시계열 특성을 활용한 다양한 이상 거래 탐지
딥러닝 모델 개발과 성능 분석

TGN의 시간순 거래 처리 (2)



시계열 특성을 활용한 다양한 이상 거래 탐지
딥러닝 모델 개발과 성능 분석

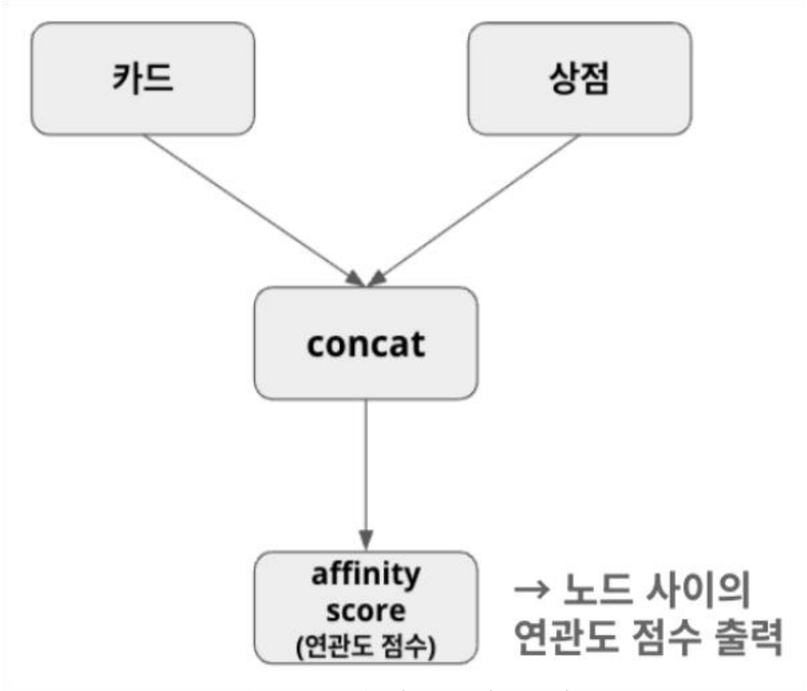
TGN의 시간순 거래 처리 (3)



시계열 특성을 활용한 다양한 이상 거래 탐지
딥러닝 모델 개발과 성능 분석

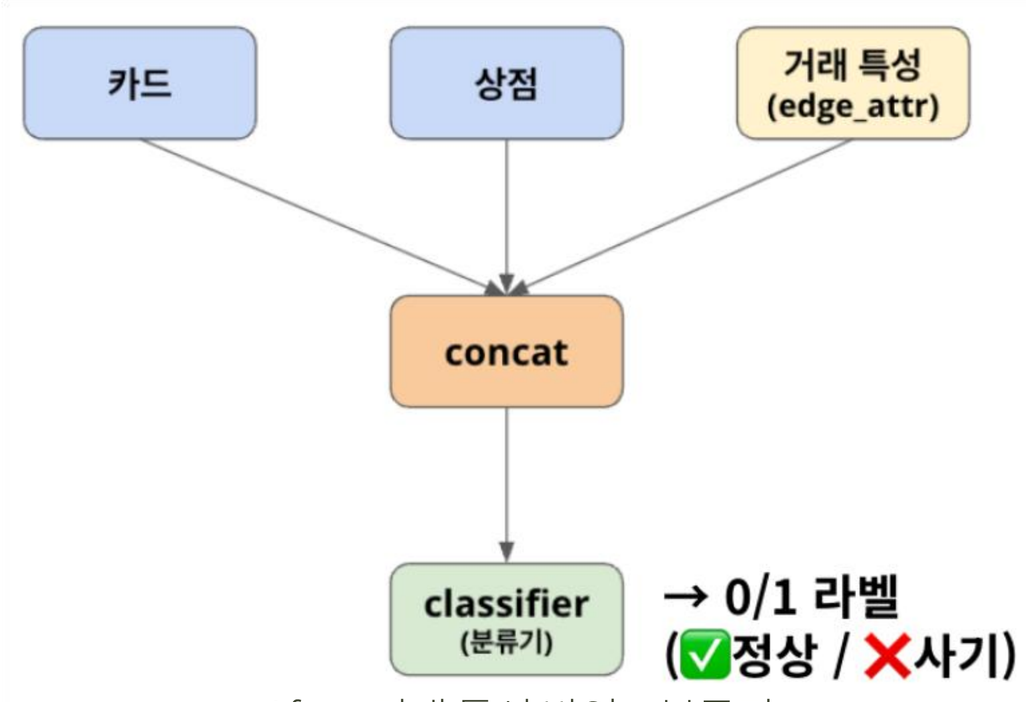
Affinity score에서 Classifier로: TGN 사기 거래 탐지 성능 개선

Before



Before: 연관도 점수만
→ 사기 여부 분류에 한계

After

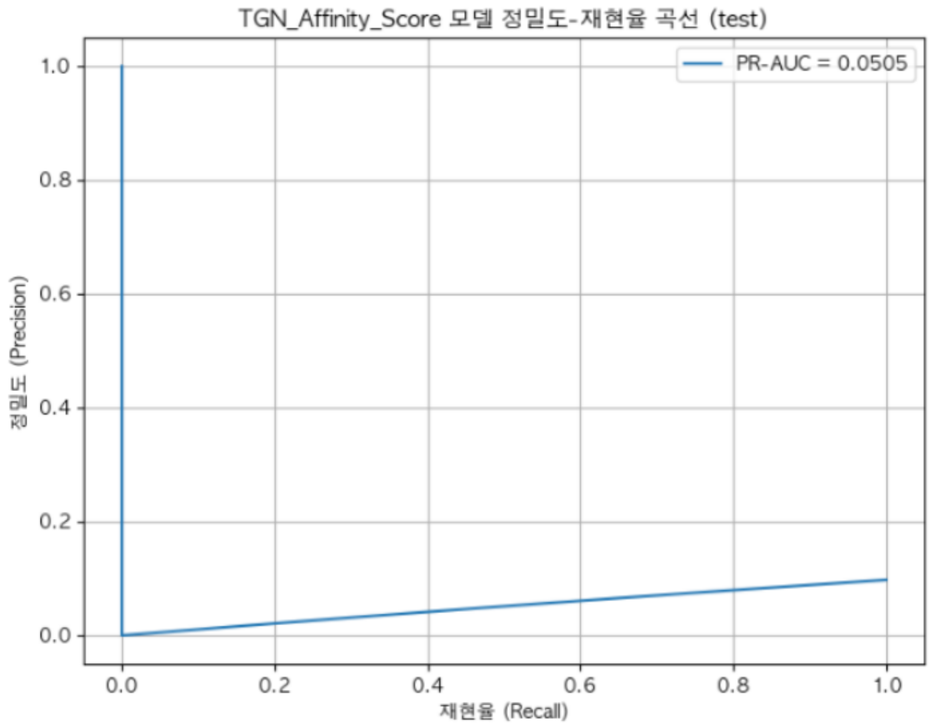


After: 거래 특성 반영 + 분류기
→ 성능 향상

시계열 특성을 활용한 다양한 이상 거래 탐지 딥러닝 모델 개발과 성능 분석

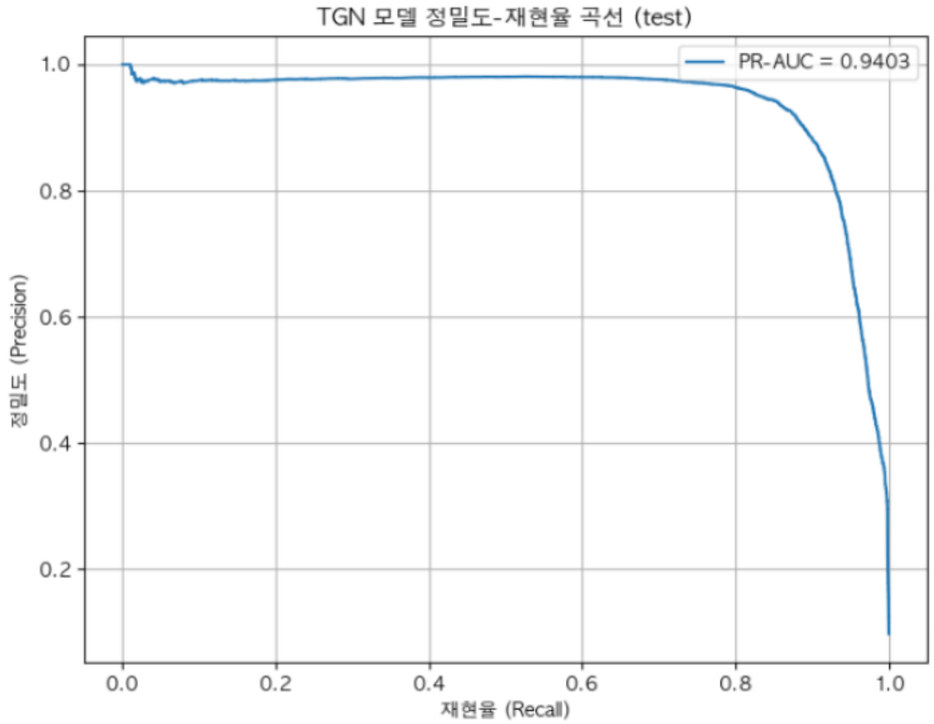
Affinity score에서 Classifier로: TGN 사기 거래 탐지 성능 비교

Before



Before: Fraud F1-score 0.1778
(탐지 성능 거의 없음)

After



After: Fraud F1-score 0.8478
(탐지 성능 대폭 향상)

시계열 특성을 활용한 다양한 이상 거래 탐지
딥러닝 모델 개발과 성능 분석

HTGN 구조

노드

고객(Customer), 카드(Card), 거래(Transaction, 트랜스포머 임베딩), 상점(Merchant)

엣지

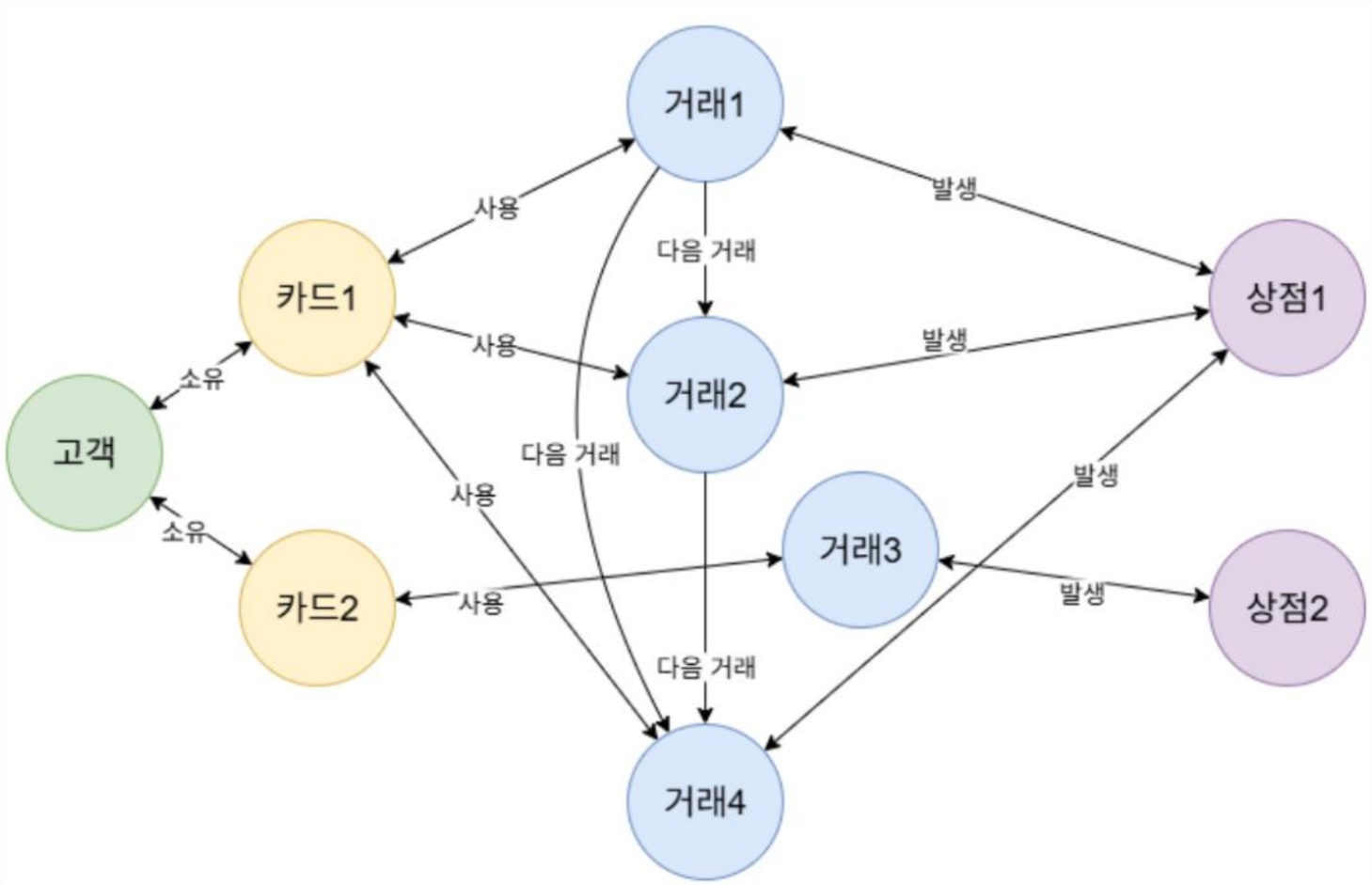
고객 ↔ 카드: 고객과 카드의 소유 관계 (양방향)

카드 ↔ 거래: 카드가 거래에 사용된 관계 (양방향)

거래 ↔ 상점: 거래가 발생한 상점 관계 (양방향)

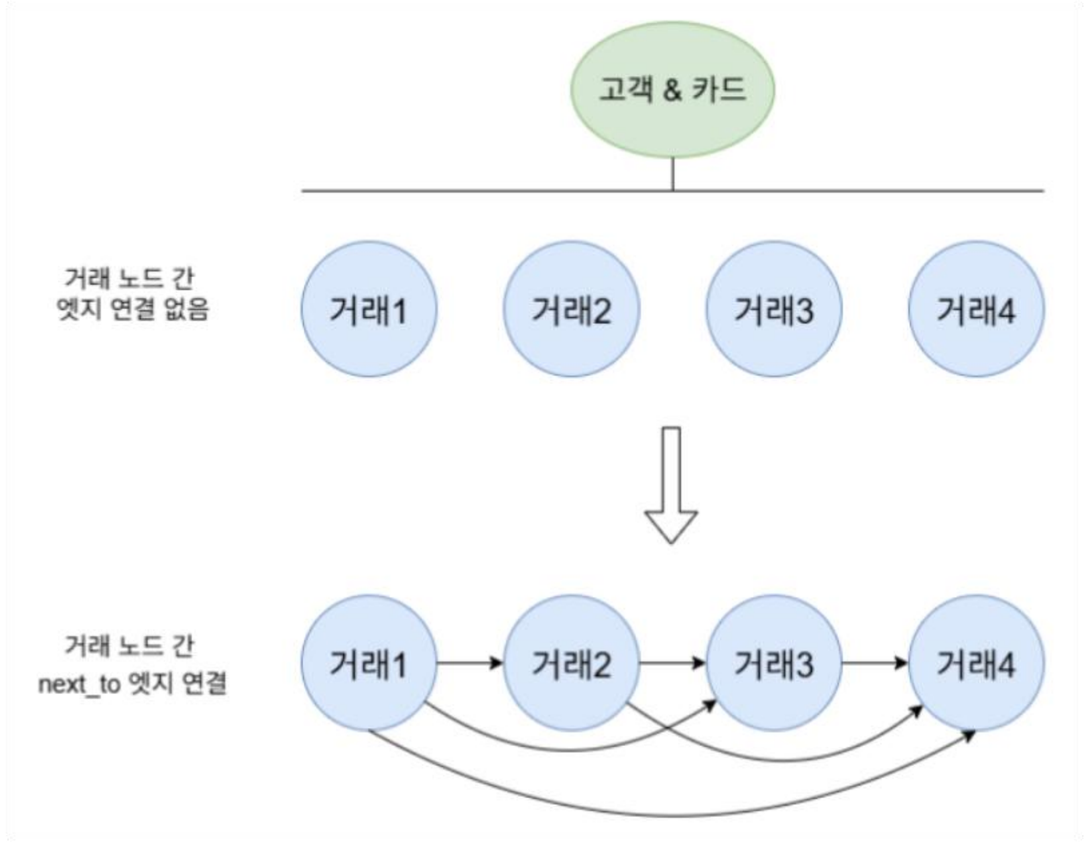
거래 → 거래: 동일 고객의 거래 노드간 시계열 순서 관계 (단방향, next_to 엣지)

HTGN 모델 및 엣지 구성도



시계열 특성을 활용한 다양한 이상 거래 탐지
딥러닝 모델 개발과 성능 분석

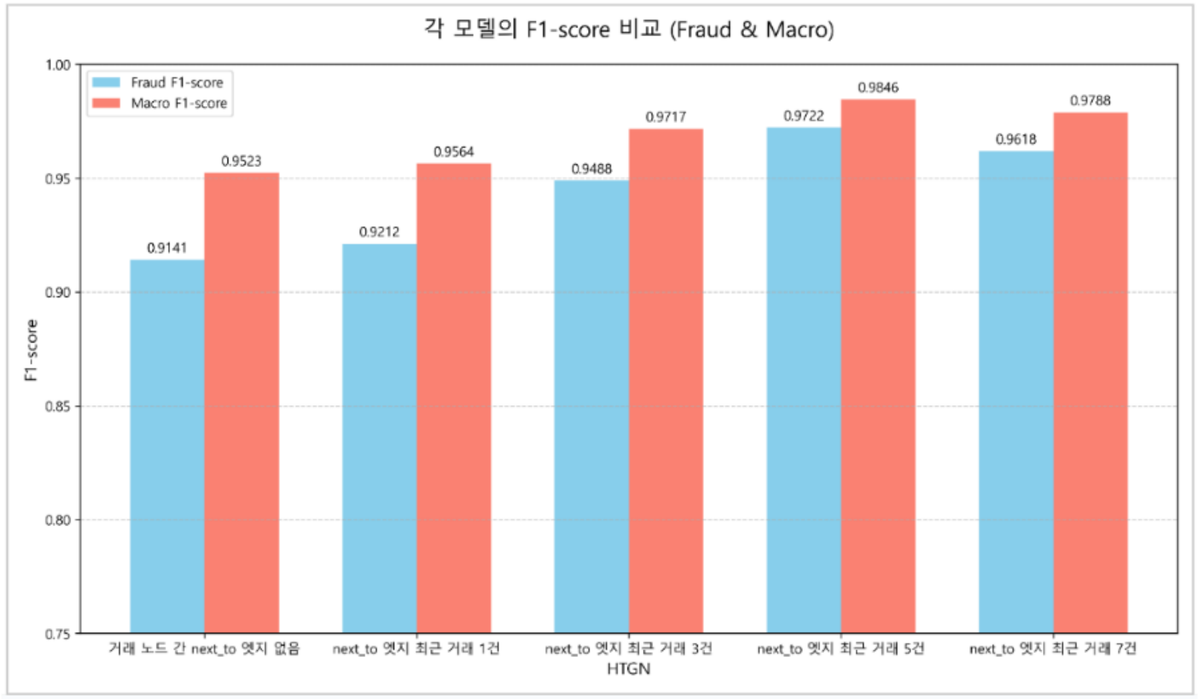
HTGN next_to 엣지 아이디어



거래 노드 간 시계열 관계를 명시적으로 반영

- 기존: 트랜스포머 임베딩만 사용 → 간접적 시계열 정보
- 개선: 거래 노드 간 next_to 엣지 추가

HTGN 거래 노드 연결 수에 따른 성능 변화



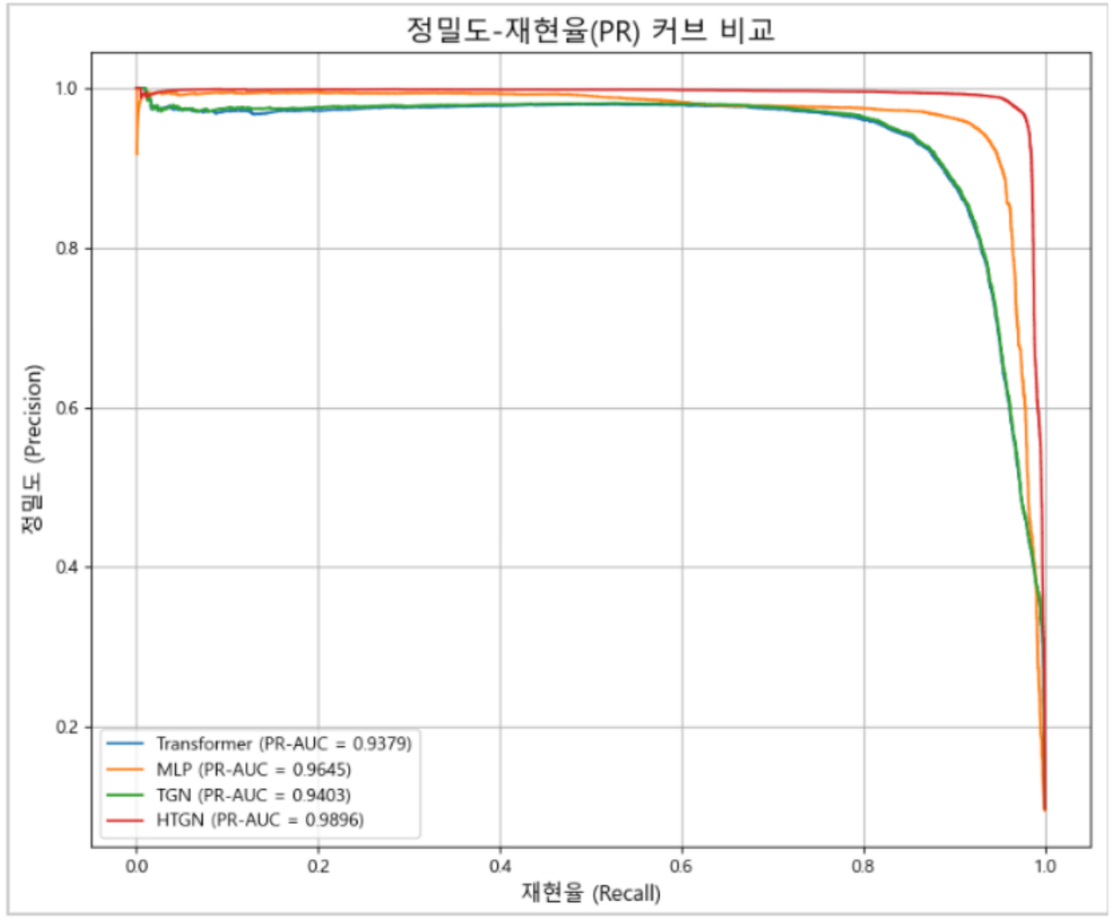
- next_to 엣지 최대 연결 개수 제한을 1 → 3 → 5 → 7로 점진적으로 높여가며 테스트 성능 비교

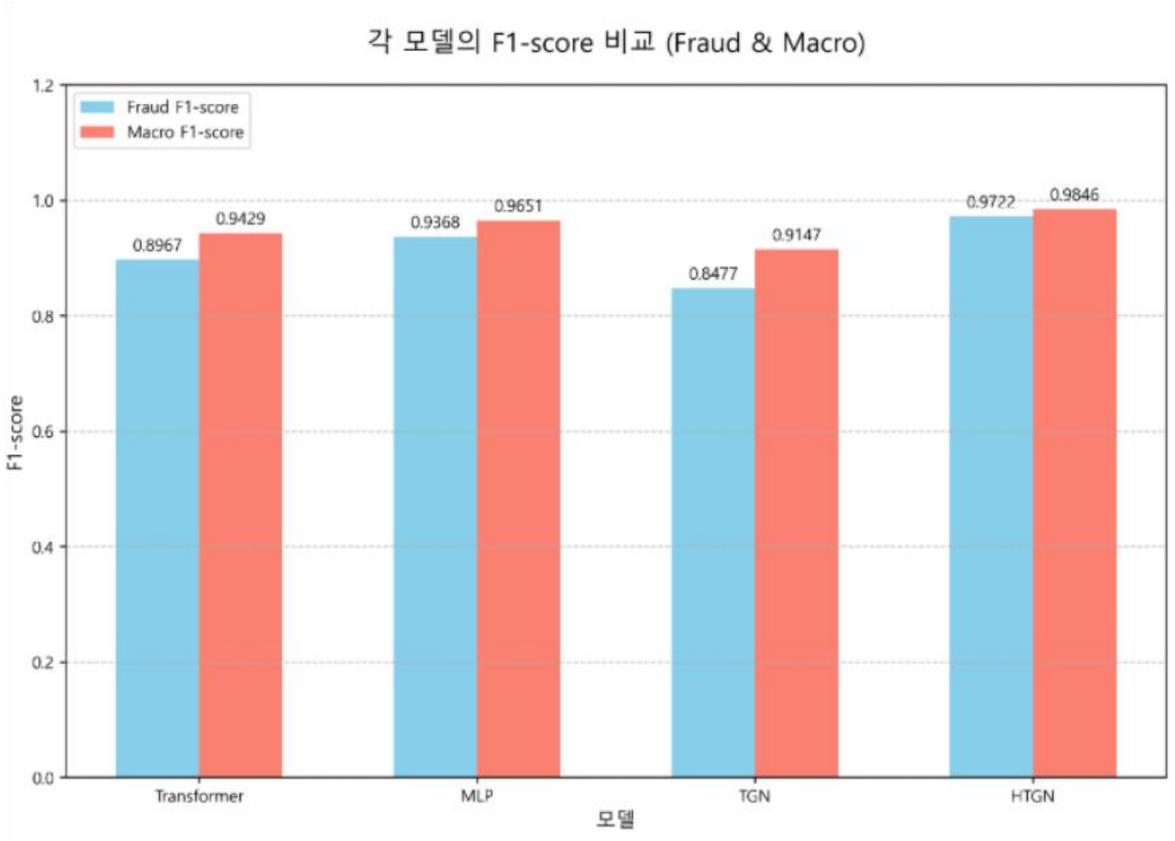
- 이상 거래 탐지 성능 점진적 향상, 5개 연결에서 최고 F1-score

- 5 → 7로 연결 증가 시 성능 소폭 감소 ⇒ 최종 설정: 5

시계열 특성을 활용한 다양한 이상 거래 탐지 딥러닝 모델 개발과 성능 분석

모델별 이상 거래 탐지 성능 비교





시계열 특성을 활용한 다양한 이상 거래 탐지 딥러닝 모델 개발과 성능 분석

요약

모델	데이터 활용	성능 특징
트랜스포머	거래 시계열	정상 거래 분류에는 강점 사기 탐지 재현율↓
MLP	거래 임베딩 + 고객·카드 프로필	전반적인 예측 성능 향상
TGN	거래 임베딩 + 그래프 (고객·카드 포함)	사기 탐지 재현율↑ / 정밀도↓ (오탐↑)
HTGN	거래 임베딩 + 이종 노드 간 관계 반영 + 노드 간 시계열 연결 강화	전반적인 예측 성능 향상 오탐·미탐 최소 / 신뢰성 가장 높음

시계열 특성을 활용한 다양한 이상 거래 탐지 딥러닝 모델 개발과 성능 분석