BGP라우팅 데이터 분석 LLM 기술 개발 – 문제정의서

20학번 손봉우, 20학번 양준혁

지도 교수님 : 이영석 교수님

목차

연구 개발의 필요성

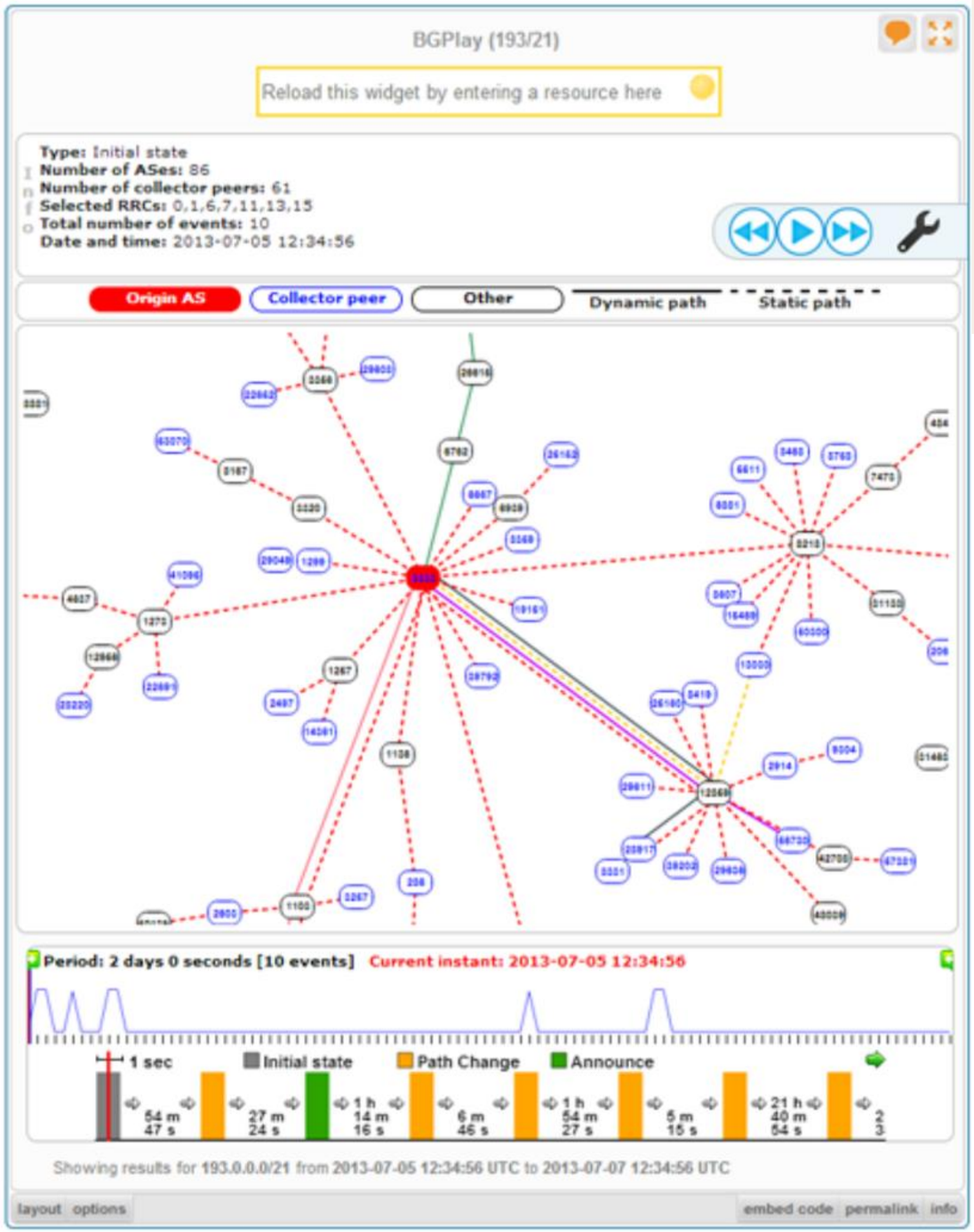
문제점 및 개선 포인트

- BGP는 인터넷 경로 설정의 핵심 프로토콜
- 설계상 보안 취약점 존재 → 장애/보안 사고 발생
  - 인증 절차 없음 -> 경로 하이재킹
  - 잘못된 경로 광고로 대규모 장애 발생 가능
- 기존 대응책(RPKI 등)은 도입률 낮고, 실시간 탐지 한계 있음
- 자연어 기반 실시간 분석 시스템의 필요성 제기

문제 정의 및 목표

문제점 및 개선 포인트

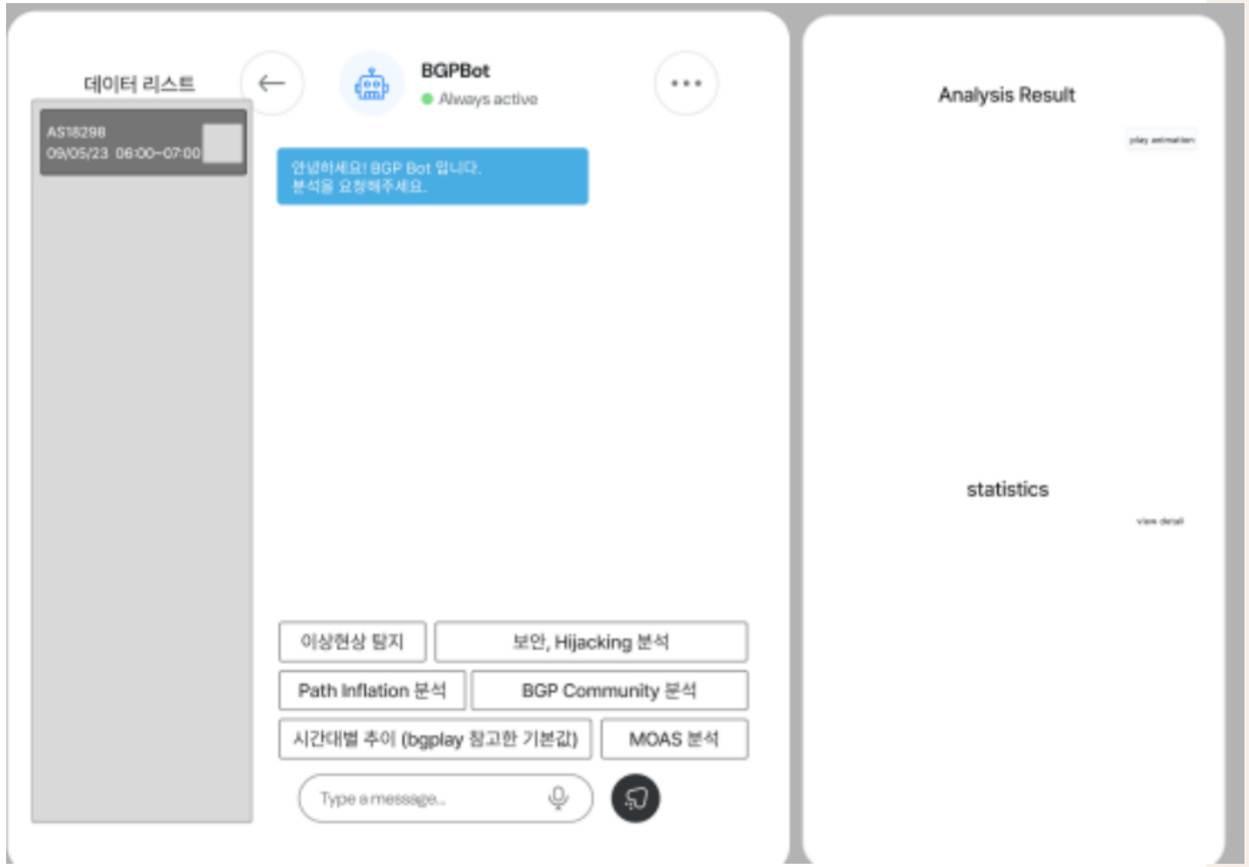
- 기존 BGP 분석 도구의 한계
  - CLI 기반 → 초보자 진입장벽
  - 실시간 분석 어려움
  - 시각화 미흡



문제 정의 및 목표

제안하는 목표

- 자연어로 BGP 데이터 분석
- 실시간 이상 감지 및 자동 경고
- 시각화 대시보드 제공



주요 기능 소개

- 자연어 질의 분석
- 시각화 대시보드
  - 경로 변화, 지리 시각화, 트래픽 히트맵
- 실시간 이상 탐지
  - 이상 패턴 인식
  - 자동 알림, 보고서 생성

- 과거 데이터 분석
- 챗봇 인터페이스
  - 초보자도 손쉽게 분석 가능

이해 당사자 인터뷰

- BGP 도구의 부적합성 -> 명령어 기반, 시각화 부족, 실시간 분석 부족
- 과거 데이터 분석 -> 복원 기능 부족, 특정 시간대 지점 복원 필요
- BGP 이상 감지 시스템 -> 일부 시스템 존재, 탐지율 낮음, 알람의 과도한 발생
- 자연어 기반 시스템의 이점 -> 초보자나 협업 부서와의 활동에 큰 도움 될 것
- 이상 징후 발생 시 가장 필요한 기능 -> 빠른 경고, 원인 요약 리포트 등
- 이상 탐지 및 분석에 자동화의 필요성 -> 반복 업무가 많아 자동화가 반드시 필요

기대 효과 및 확장 가능성

기대 효과

- 사용자 진입 장벽 제거
- 실시간 이상 탐지로 보안 강화
- 네트워크 운영 효율성 개선

확장 가능성

- OSPF, IS-IS 등 라우팅 프로토콜 추가
- AUTO-NOC 시스템 개발
- XDR/SIEM 연동 API 서비스화

연구 개발의 추진 전략 및 방법

추진 전략 개요

AGILE 방식으로 사용자 요구를 반영하며 반복적으로 개발. 초기에는 전문가 인터뷰를 통해 문제를 정의하고, 이후 역할 분담을 통해 자연어 질의 처리, 시각화, 이상 탐지 기능을 순차적으로 구현. 각 단계별로 프로토타입을 개선하며, 최종적으로 통합 테스트와 발표 준비를 진행할 예정.

연구 개발의 추진 전략 및 방법

학기별 추진 일정

🗓️ 학기별 주차별 일정표

주차	주요 내용
1~2주차	프로젝트 기획 및 문제 정의, 인터뷰/설문 조사
3~5주차	시스템 구조 설계, 기술 검토
6~9주차	데이터 수집 및 자연어 처리 기능 개발
10~13주차	실시간 이상 탐지, 시각화 대시보드 구현
14~15주차	통합 테스트, 발표자료 제작 및 마무리

Q&A

감사합니다.

20학번 손봉우, 20학번 양준혁