차세대 5G네트워크 보안을 위한 LLM 및 RAG 기반 공격 시나리오 생성

하유성, 김기천*

건국대학교

everna12@konkuk.ac.kr, *kckim@konkuk.ac.kr

Study of LLM and RAG-based Attack Scenarios for Next-Generation 5G Network Security

Ha Yu Seong, Kim Kee Cheon*

Konkuk Univ.

요 약

본 논문은 LLM 및 RAG 기술을 이용하여 5G 네트워크 환경에서 발생할 수 있는 다양한 공격 시나리오 생성을 자동화하고, 네트워크 시뮬레이션 도구를 통해 테스트하여 나온 결과를 평가하고 분석하여 네트워크 취약성과 기존 보안 프레임워크에 대한 보안을 강화하는 방법론을 소개했다. 제안된 방법론은 공격 시나리오 생성을 자동화할 뿐만 아니라 현실적인 네트워크 동작과 잠재적인 위협 패턴을 기반으로 함으로써 네트워크 보안 관리에 있어 사전에 예방할 수 있고, 보다 효과적으로 예측하여 완화할 수 있다.

Ⅰ. 서 론

최근 몇 년간 사물 인터넷(IoT), 클라우드 서비스와 같은 통신 기술이 빠르게 성장하면서 네트워크 트래픽이 급격히 증가하고 있다. 이러한 수요 증가는 더 높은 데이터 처리량과 감소된 대기 시간을 지원할 수 있는 고급 네트워크 프레임워크의 필요성을 강조한다[1]. 5G 기술은 더 빠른 속도, 더 낮은 대기 시간, 수많은 장치 간의 대규모 연결이 가능하게 함으로써 이러한 요구 사항을 해결한다[2]. 결과적으로 증가하는 네트워크 트래픽을 효과적으로 관리하기 위해서는 5G 네트워크의 구축이 점점 더 중요해지고 있다.

그러나 새로운 기술의 등장과 복잡한 네트워크 아키텍처로 인해 더 많은 공격 가능성이 생기기 때문에 보안 위험 또한 높아진다[3, 4]. 예를 들어, 분야와 목적별로 분리되어 폐쇄적이었던 기존의 네트워크 구조와 달리, 5G는 개방형으로 설계되어 용도에 따른 분산 구조로 대역을 쪼개 여러 분야에 적용하는 네트워크 슬라이싱 방식으로 인해 보안에 취약점을 발생시킨다[5]. 이를 고려하였을 때 기존의 네트워크에서 사용되는 보안 솔루션보다 더 안전하고 발전된 보안 전략이 필요하다. 하지만 큰 발전에 따라 발생할 수 있는 다양한 상황에 대한 공격 시나리오를 수동으로 생성하는 것은 많은 시간과 노력이 필요하며, 소프트웨어 기능과 기본 도메인에 대한 깊은 이해가 필요하다[6].

이러한 과제를 해결하기 위해 본 논문에서는 네트워크 보안 프레임워크를 강화하기 위해 LLM(Large Language Model) 및 RAG(Retrieval-Augmented Generation) 기술을 이요하여 인공 지능의 발전을 활용하는 새로운 방법론을 제안한다. 본 연구는 공격 시나리오 생성을 자동화하고 시뮬레이션을 통해 5G 네트워크에 대한 잠재적 영향을 평가함으로써 효과적이고 효율적인 보안 솔루션을 개발할 수 있을 것으로 생각한다.

Ⅱ. 본론

LLM을 적용할 때의 중요한 과제 중 하나는 할루시네이션(Hallucination) 문제가 있다. 할루시네이션 문제란 모델이 특정 주제에 대해서 맥락과 관련이 없거나, 거짓된 정보를 마치 옳은 답처럼 생성해 내는 현상이다. 할루시네이션의 발생 원인은 학습한 데이터의 정보 부족, 학습 데이터의 낮은 품질 등이 있다. 이러한 문제를 보완하기 위해서 특정 도메인에 대한 데이터를 추가로 학습하는 파인 튜닝(Fine Tuning)과 프롬프트와 외부 지식 기반에 접근함으로써 필요 정보를 활용하여 더 정확하고 신뢰성 있는 결과물을 생성하는 RAG 기술이 있다[7, 8, 9].

먼저 할루시네이션 문제로 인해 실제 위협을 나타내지 않거나 비현실적인 공격 시나리오가 생성될 수 있다. 이를 완화하기 위해 파인 튜닝 기술을 활용하여 LLM을 CVE, 과거 공격 사례 등을 데이터 셋으로 하여 LLM이 컴퓨터 보안과 5G와 관련된 도메인 지식을 학습함으로써 더 효과적으로 공격 시나리오를 생성해 낼 수 있다. 그리고 5G-NIDD, 5G-PFCP, 5GAD-2022와 같은 5G 네트워크 환경에서 수집된 데이터 셋은 5G에 특화되어 있기 때문에 현실적인 네트워크 트래픽, 공격 벡터 및 이상 현상을 제공하기 때문에 이러한 데이터 셋은 RAG 시스템의 외부 지식 기반에 저장한다[10]. 이를 통해 모델은 생성 프로세스 중에 특정 네트워크 시나리오 및 알려진 취약점에 대한 관련 정보를 가져올 수 있다[11].

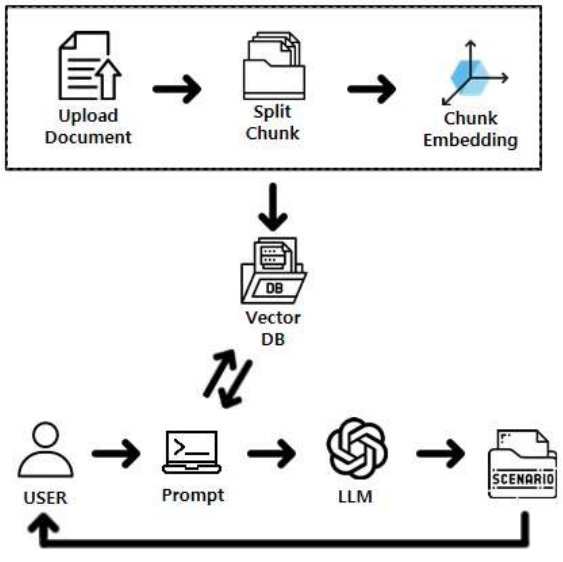

그림 1. 시나리오 생성 아키텍처

그림 1은 LLM과 RAG 기술을 이용하여 시나리오를 생성하는 프레임워크이다. 먼저 사용자가 5G-NIDD, 5G-PFCP, 5GAD-2022와 같은 데이터 셋들을 청크 단위로 분할한다. 청크는 보통 문장 또는 문단과 같은 작은 텍스트 조간을 의미하며, 이 청크들을 통해 정보 검색에 활용한다. 생성된 청크들을 임베딩하여 벡터 형태로 변환하는 과정을 거친다. 이렇게 임베딩된 청크들을 기반으로 벡터 데이터베이스를 구축하게 된다. 그다음 사용자는 생성하고자 하는 시나리오와 관련된 프롬프트를 작성하게 되고, 관련 정보를 벡터 데이터베이스에서 적절한 청크를 검색하게 된다. 그렇게 검색된 정보와 프롬프트를 기반으로 LLM의 입력 데이터로 사용되고, 파인튜닝된 LLM을 통해 공격 시나리오를 생성하게 된다.

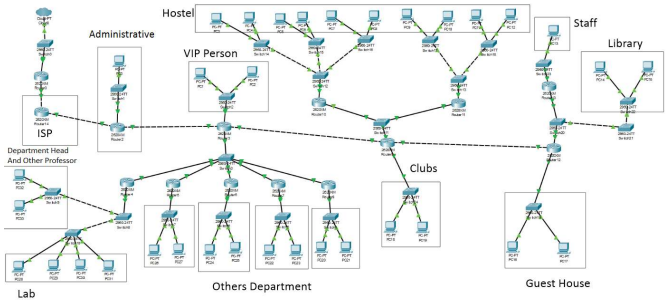

그림 2. 시나리오 기반 구현 예시

그림 2는 생성된 시나리오를 바탕으로 구현 가능한 예시이다[12]. NS3, OMNeT++, GNS3와 같은 네트워크를 모델링하여 시뮬레이션할 수 있는 도구를 사용하여 가상 환경에서 구축하게 된다. 구축된 이 환경에서 LLM을 통해 생성된 시나리오에 대해 공격과 네트워크 응답에 대한 시뮬레이션을 진행하고, 네트워크 장애 시간, 데이터 침해 정도, 시스템 리소스 사용 등 여러 방면에서 시나리오에 관한 결과를 분석한다.

Ⅲ. 결론

본 논문에서는 빠르게 진화하는 5G 네트워크 환경에서 발전된 보안 솔루션의 필요성과 기존의 수동 시나리오 생성의 문제점을 제기했다. LLM 및 RAG 기술을 활용하여 이러한 네트워크 환경에서 발생 가능한 공격 시나리오 생성을 자동화한 후, 생성된 시나리오를 네트워크 시뮬레이션 도구를 통해 테스트하여 나온 결과를 평가하고 분석하여 네트워크 취약성과 기존 보안 프레임워크에 대한 보안을 강화하는 방법론을 소개했다.

제안된 방법론은 공격 시나리오 생성을 자동화할 뿐만 아니라 현실적인 네트워크 동작과 잠재적인 위협 패턴을 기반으로 하도록 보장함으로써 네트워크 보안 관리에 있어 사전에 예방할 수 있고, 보다 효과적으로 예측하고 완화할 수 있다.

추후 필요한 연구 과제로 실제 네트워크 환경에서 직접 구현을 통해 제안된 보안 강화의 실제 성능과 실용성에 대한 평가가 필요하다. 또한, LLM이 알려진 취약성뿐만 아니라 이전에 알려지지 않은 새로운 보안 위협에 대한 취약점 및 시나리오를 파인튜닝과 RAG를 통해 생성이 가능한지 연구하는 것도 중요하다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 디지털선도기술 핵심인재양성사업의 연구결과로 수행되었음 (IITP-2024-2020-0-01834)

참 고 문 헌

[1] Salahdine, Fatima, Tao Han, and Ning Zhang. "Security in 5G and beyond recent advances and future challenges." Security and Privacy 6.1 (2023): e271.

[2] Wang, Zihao, Kar Wai Fok, and Vrizlynn LL Thing. "Exploring Emerging Trends in 5G Malicious Traffic Analysis and Incremental Learning Intrusion Detection Strategies." arXiv preprint arXiv:2402.14353 (2024).

[3] Tyokighir, Silas Soo, et al. "New developments and trends in 5G technologies: applications and concepts." Bulletin of Electrical Engineering and Informatics 13.1 (2024): 254-263.

[4] 박태근, 박종근, & 김기원. (2022). Analysis of the IP Spoofing Attack Exploiting Null Security Algorithms in 5G Networks. 한국컴퓨터정보학회논문지, 27(9), 113-120.

[5] Wala, Fatema Bannat, and Mariam Kiran. "5G Network Security Practices: An Overview and Survey." arXiv preprint arXiv:2401.14350 (2024).

[6] Jung, Hyunggu, et al. "Toward value scenario generation through large language models." Companion Publication of the 2023 Conference on Computer Supported Cooperative Work and Social Computing. 2023.

[7] Tonmoy, S. M., Zaman, S. M., Jain, V., Rani, A., Rawte, V., Chadha, A., & Das, A. (2024). A comprehensive survey of hallucination mitigation techniques in large language models. arXiv preprint arXiv:2401.01313.

[8] 정천수. (2023). LLM 애플리케이션 아키텍처를 활용한 생성형 AI 서비스 구현: RAG 모델과 LangChain 프레임워크 기반. 지능정보연구, 29(4), 129-164.

[9] 조찬영, 강성준, & 정현준. (2023, November). RAG 기반 랭체인을 이용한 생성형 AI 챗봇 구현. In Proceedings of KIIT Conference (pp. 460-463).

[10] 장지호 외. "5G 네트워크 침입 탐지를 위한 데이터셋 및 연구 동향 조사." 한국정보과학회 학술발표논문집, 2023, 1166-1168.

[11] Arora, Chetan, Tomas Herda, and Verena Homm. "Generating Test Scenarios from NL Requirements using Retrieval-Augmented LLMs: An Industrial Study." arXiv preprint arXiv:2404.12772 (2024).

[12] Mohammad, Chowdhury & Masum Refat, Chowdhury & Tarek, Rabiul & Rashid, Syed Zahidur & Rashid, Abdul & Gafur,. (2018). Design and Performance Investigation of Campus Area Network (CAN) Based on Different Routing Protocols.