5G-Advanced를 위한 N2/N3 인터페이스 DoS 공격 영향 분석

박재형[1], 이종혁[2]
[1]세종대학교 정보보호학과 & 지능형드론 융합전공 석사과정
[2]세종대학교 정보보호학과 & 지능형드론 융합전공 교수
jaehyoung@pel.sejong.ac.kr, jonghyouk@sejong.ac.kr

Impact Analysis of DoS Attacks on N2/N3 Interfaces in a 5G-Advanced Core Network

Jaehyoung Park[1], Jong-Hyouk Lee[2]
[1.2]Dept. of Computer and Information Security & Convergence Engineering for Intelligent Drone, Sejong University

요 약

이동통신 분야 사실표준화 기구인 3GPP(3rd Generation Partnership Project)에서는 기존의 5G 이동통신 기술을 향상시키기 위한 5G-Advanced 연구를 시작했다. 5G 및 5G-Advanced 시대에 접어들면서 네트워크를 향상시키기 위한 다양한 요소기술들이 등장하였지만, 이러한 기술 변화에 비례하여 네트워크를 위협하는 공격 표면들이 증가할 것으로 예상된다. 점진적인 네트워크 보안 위협에 대응하기 위해 보안 기술은 에드온(Add-on) 형태로 개발되었지만, 이는 이동통신시스템에서 보안 기술의 신뢰성을 낮추고 네트워크에 대한 보안 품질을 보장하지 못한다. 따라서, 본 논문에서는 5G-Advanced에서 사용되는 N2/N3 인터페이스에서 발생가능한 DoS(Denial of Service) 공격에 대해 실험하고 분석한다. 분석 결과는 5G-Advanced 이동통신시스템의 공격 표면을 나타내고 보안 내재화의 필요성을 강조한다.

1. 서론

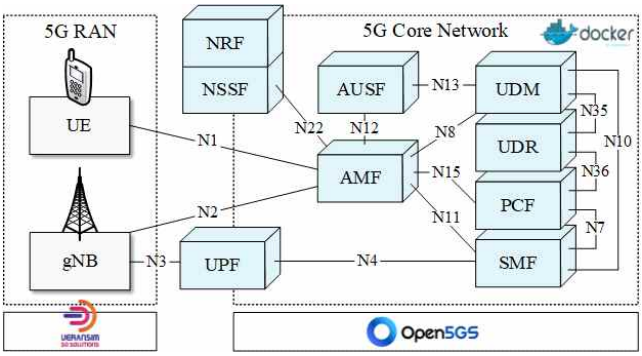
현대의 이동통신기술 아키텍처는 다양한 트래픽과 요구사항의 증가로 인해 네트워크의 유연성, 확장성 그리고 배포에 대한 포괄적인 기능을 제공해야 한다. 5G-Advanced 시대에 들어서면서 이러한 요구사항을 충족시키기 위해 MEC(Multi-Access Edge Computing), 네트워크 슬라이싱, SDN(Software Defined Networking)/NFV(Network Function Virtualization) 등과 같은 다양한 요소기술들이 연구되고 있다. 해당 요소기술들은 5G 이상의 네트워크에서 사용자의 요구사항을 충족시키는 QoS(Quality of Service)를 제공할 수 있도록 한다[1].

5G-Advanced 시스템은 지속적으로 표준화되고 있고 개발자들은 이미 오픈소스를 기반으로 개방화된 네트워크를 사용자들에게 제공하고 있다. 하지만, 5G-Advanced의 발전은 새로운 신뢰성과 보안위협에 관한 문제를 야기할 수 있다[2]. 특히, 기존 이동통신 시스템에서도 흔히 발생하였던 DoS 공격은 차세대 이동통신시스템에서도 서비스의 지연을 발생시키고 사용자의 요구사항과 QoS를 보장할 수 없게 만든다. 즉, 이동통신시스템에서 5G-Advanced 요소기술들이 제 기능을 상실하여 다양한 서비스를 제공할 수 없게 된다. 이로 인해, 5G-Advanced 보안 위협에 대응하기 위한 다양한 보안 기술들이 요구되는 실정이다. 기존의 이동통신시스템에서는 보안 기술을 에드온 형태로 개발하였으나, 이는 보안 기술의 신뢰성을 낮추고 5G-Advanced에 대한 보안 품질을 보장하지 못하게 할 수 있다. 따라서, 안전한 5G-Advanced 네트워크를 구성하기 위해서는 표준화 단계에서부터 보안 내재화를 위한 연구가 필요한 시점이다.

따라서, 사전에 5G-Advanced 이동통신시스템에서 발생가능한 보안 위협을 식별하고자 5G부터 새롭게 정의된 N2/N3 인터페이스에 대한 DoS 공격을 실험한다. N2/N3 인터페이스는 코어 네트워크 외부와 연결된 인터페이스이므로 DoS 공격 지점이 될 수 있기 때문에, 본 논문은 5G-Advanced 네트워크의 공격 표면을 식별하고 보안 내재화의 필요성을 강조한다[3].

2. N2/N3 인터페이스 DoS 공격 실험 및 분석

N2/N3 인터페이스에 대한 DoS 공격을 실험하기 위해 (그림 1)과 같은 실험환경을 활용한다. 해당 실험환경은 오픈소스를 기반으로 구성하였으며, 이동통신시스템을 위한 코어 네트워크, RAN(Radio Access Network)으로 구성된다. 코어 네트워크는 Open5GS 오픈소스를 활용하였으며, 도커 컨테이너 기반의 NF(Network Function)들이 동작한다. RAN은 UERANSIM 오픈소스를 활용하였으며, 5G 기지국(gNB)과 5G UE를 에뮬레이션할 수 있게 한다[4][5].



(그림 1) 실험환경 구성도

(그림 1)의 실험환경은 5G 및 5G-Advanced 네트워크에서 사용되는 일반적인 구성요소와 인터페이스를 반영하고 있다. 코어 네트워크는 이동통신시스템에서 발생하는 CP(Control Plane)와 UP(User Plane)를 처리하고, gNB는 UE에게 무선 인터페이스를 제공함으로써 UE가 인터넷을 사용할 수 있도록 한다. 이중 본 논문에서 실험하고자 하는 N2/N3 인터페이스는 이동통신시스템의 핵심인 코어 네트워크와 연결되는 외부 인터페이스이다.

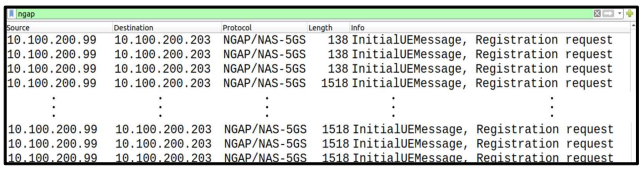
N2 인터페이스는 코어 네트워크 내부 NF인 AMF(Access and Mobility Management Function)와 gNB 사이의 인터페이스이다. AMF는 코어 네트워크 내부에서 UE 등록 및 이동성 관리를 위한 기능을 제공하며, gNB는 UE가 이동통신 서비스를 이용할 수 있도록 무선 링크를 제공한다. 해당 인터페이스에서는 5G부터 새롭게 정의된 NGAP(Next Generation Application Protocol)가 사용된다.

N3 인터페이스는 UPF(User Plane Function)와 gNB 사이의 인터페이스이다. UPF는 코어 네트워크 내부에서 UP 데이터를 처리하는 역할을 담당하며, gNB와 데이터 네트워크 사이에서 사용자 패킷을 라우팅하여 전송한다. 이를 통해 UE와 데이터 네트워크 간의 연결성을 제공하여 인터넷 서비스를 이용할 수 있게 한다. 두 인터페이스는 모두 UE에게 이동통신 서비스를 제공하기 위해 사용되지만, 코어 네트워크를 위협할 수 있는 공격 지점으로 활용될 수 있다.

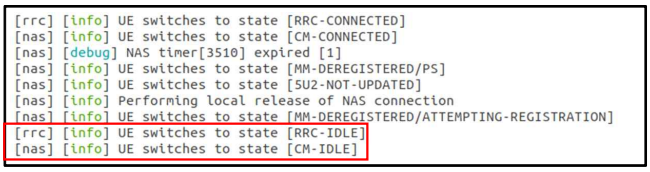
본 논문의 N2 인터페이스 DoS 공격은 CP에서 사용되는 NGAP 프로토콜을 악용하고 N3 인터페이스 DoS 공격은 UP에서 흔히 사용되는 UDP(User Datagram Protocol)를 악용한다.

N2 인터페이스 DoS 공격에서는 NGAP 프로토콜에서 사용되는 초기 UE 등록 메시지를 악용한다. 해당 메시지는 UE가 처음 이동통신 네트워크에 등록될 때, gNB가 AMF에 전송하는 메시지이다. N2 인터페이스 DoS 공격에서는 gNB가 AMF에게 대량의 초기 UE 등록 메시지를 전송한다.

N2 인터페이스 DoS 공격의 결과는 AMF가 과부하된다. 이로인해 새로운 UE가 등록을 원할 경우, 서비스를 제공할 수 있는 AMF가 과부하되어 타임아웃되거나 등록 서비스를 지원하는 AMF를 발견하지 못해 UE가 이동통신시스템에 등록되지 못하는 결과를 초래할 수 있다. 해당 DoS 공격 시나리오에서 공격자는 허위 기지국으로 간주될 수 있다.



(그림 2) N2 인터페이스 DoS 공격 패킷

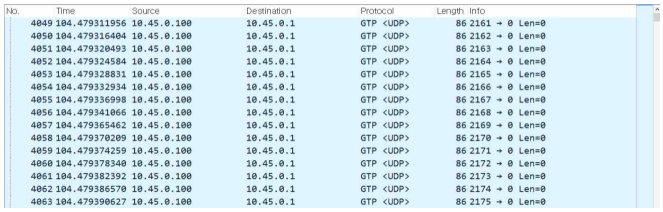


(그림 3) N2 인터페이스 DoS 영향 (UE 등록 실패)

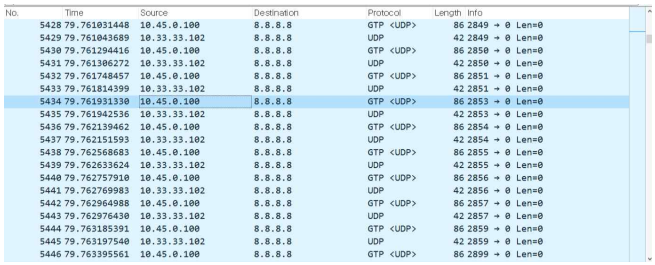
N3 인터페이스 DoS 공격은 UP에서 흔히 사용될 수 있는 UDP 패킷을 사용한다. UDP는 사용자가 인터넷을 사용할 때 흔히 사용되는 패킷으로 UE는 UDP 패킷을 gNB에게 전송한다. gNB는 수신한 UDP 패킷을 GTP(GPRS Tunnelling Protocol)로 캡슐화하여 N3 인터페이스를 통해 UPF에게 전송한다. UPF는 수신된 GTP 패킷을 역 캡슐화하고 UE가 원하는 대상으로 UDP 패킷을 라우팅한다.

N3 인터페이스 DoS 공격의 대상은 UP 데이터를 처리하는 UPF와 데이터 네트워크에 존재하는 DNS(Domain Name Server)를 대상으로 한다. N3 인터페이스 DoS 공격 결과는 UPF의 CPU(Central

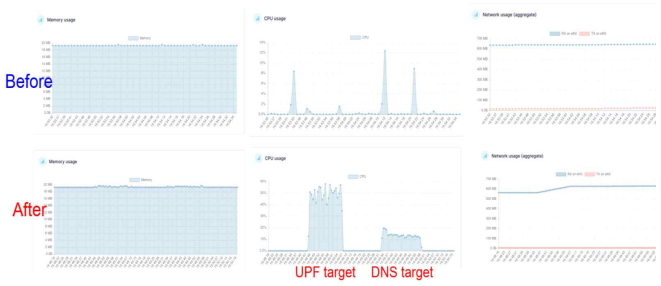
Processing Unit) 사용량, 메모리 사용량, 네트워크 사용량을 증가시켰다. 이는, UPF를 통해 동일한 네트워크에서 이동통신 서비스를 제공받는 UE들이 인터넷을 이용하는 데 있어 서비스 지연이 발생함을 의미한다. 해당 DoS 공격 시나리오에서 공격자는 악성 UE 혹은 허위 기지국으로 간주 될 수 있다.



(그림 4) N3 인터페이스 DoS 패킷 (타겟: UPF)



(그림 5) N3 인터페이스 DoS 패킷 (타겟: DNS)



(그림 6) N3 인터페이스 DoS 영향 (UPF 사용량 증가)

본 논문의 N2/N3 인터페이스 DoS 공격 실험 결과를 통해 해당 인터페이스에서 발생하는 DoS 공격은 5G-Advanced 이동통신시스템에 악영향을 미칠 수 있음을 분석하였다. 다양한 요소기술들이 융합되어 사용자에게 더 높은 QoS 보장하고자 하는 5G-Advanced에서는 서비스에 대한 가용성이 중요시된다. 본 논문을 통해 실험된 N2/N3 인터페이스 DoS 공격은 5G-Advanced 이동통신시스템에서 공격 표면으로 작용할 수 있다. 따라서, 안전한 이동통신시스템을 구성하기 위해서는 사전에 잠재적인 보안 위협을 식별하고 다양화된 공격에 대응할 수 있는 보안 기술을 개발해야 한다.

3. 결론

본 논문에서는 5G부터 새롭게 사용되는 N2/N3 인터페이스에서의 DoS 공격을 실험하였다. N2 인터페이스에서의 DoS 공격은 CP 데이터를 악용하였고, N3 인터페이스에서의 DoS 공격은 UP 데이터를 악용하였다. 공격 결과, N2 인터페이스 DoS 공격은 이동통신시스템에서 UE 등록 서비스에 오류를 발생시켰고, 이는 잠재적으로 허위 기지국으로 인해 공격이 가능함을 분석하였다. N3 인터페이스 DoS 공격은 이동통신시스템에서 UE가 인터넷 서비스를 사용하는데 있어 서비스 지연을 발생시켰고, 이는 잠재적으로 악의적인 UE 혹은 허위 기지국에 의해 발생할 수 있음을 분석하였다.

N2/N3 인터페이스는 5G-Advanced로 계승될 것으로 예상되기 때문에 안전한 이동통신시스템 구성을 위해 5G-Advanced에 대한 공격 표면을 사전에 식별하였다. 이는 5G-Advanced 코어 네트워크 외부에서의 잠재적인 보안 위협이 발생 가능함을 나타내고 이에 대응하기 위한 보안 기술의 필요성을 강조한다. 향후 연구에서는 사전 식별된 공격들에 대응할 수 있도록 5G-Advanced에 특화된 보안 기술을 개발하고자 한다.

Acknowledgement

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00796, 상시적 보안품질 보장을 위한 6G 자율보안 내재화 기반기술 연구)

참고문헌

[1] 3GPP, 3GPP TS 23.501, “System architecture for the 5G System (5GS) Stage 2 (Release 18)”, Dec. 2023.

[2] S. Sulivan, et al., “5G security challenges and solutions: a review by OSI layers”, IEEE Access, vol. 9, pp. 116294-116314, Aug. 2021.

[3] F. Salahdine, T. Han, and N. Zhang, “Security in 5G and beyond recent advances and future challenges”, Security and Privacy, vol. 6, no. 1, Sep. 2022.

[4] Open5GS, [Online]. Available: https://open5gs.org [Accessed: 5-March-2024].

[5] UERANSIM, [Online]. Available: https://github.com/aligungr/UERANSIM, [Accessed: 5-March-2024].