4G LTE 이동통신망에서의 시그널링 DoS 탐지 기술

장웅 · 김세권 · 오주형 · 임채태

한국인터넷진흥원

The Detection of Signaling Dos on 4G LTE Cellular Network

Woung Jang · Se-Kwon Kim · Joo-Hyung Oh · Chae-Tae Im

Korea Internet and Security Agency

E-mail : {jangw2232,heath82,jhoh,chtim}@kisa.or.kr

요 약

최근 전세계적으로 이동통신 서비스는 4G로의 급격한 전환이 이루어지고 있다. 그러나 4G의 급격한 도입은 보안 위협에 따른 충분한 검토가 이루어지지 못한 채 진행되었기에 다양한 위협이 존재할 것으로 예상된다. 따라서 국외에서는 4G 망의 취약점 및 보안 위협에 대한 연구가 활발히 진행되고 있으나, 국내에서는 상대적으로 연구가 미진한 상황이다. 특히 4G 가입자가 급격히 증가한 국내 상황에서, 4G 망의 안정성 및 가용성을 저해하는 보안 위협은 다수의 사용자에게 치명적인 영향을 줄 수 있다. 4G 망을 안정적으로 보호하기 위해서는 모바일 망 특성에 대한 고려가 필요하다. 모바일 망은 한정된 무선 자원을 가지고 있으며, 이를 효율적으로 관리하기 위하여 일정 시간 동안 사용이 없는 단말의 무선 자원을 해제하고, 다시 데이터를 송수신 할 때 무선 자원을 재할당한다. 무선 자원 할당 및 해제 과정에서는 다수의 시그널링 메시지가 발생한다. 본 논문에서는 악의적으로 무선 자원 할당 및 해제 과정을 반복하여 대량의 시그널링 메시지를 유발시킴으로써 무선 자원을 관리하는 모바일 망 장비의 안정성 및 가용성을 저해하는 시그널링 DoS 트래픽을 탐지하기 위한 기술을 제안한다.

ABSTRACT

For in recently years, global cellular network service is changing rapidly to 4G. However, the fast introducing of 4G has been going with not enough research about security threat, it could be many kind of vulnerability. Therefore the research about security threat on 4G network is ongoing in external countries, but not sufficient in domestic. particularly in domestic situation of rapidly increased subscribers, The security threats which are hindering stability and usability could make a fatal effect on many users. 4G network should be considered about the feature of mobile network to protect 4G network stable. Mobile network has limited radio resources, it releases the radio resource which is not used in selected time and reallocate when detected the data transmission. Many signaling messages are transferred in the network entities to allocate or release the radio resource. In this paper, it will be introduced the technology to detect signaling DoS traffic hindering the stability and usability of network entities managing the radio resources by huge signaling message from the repetitive wireless connection/release message.

키워드

4G, LTE, 시그널링 DoS

Ⅰ. 서 론

오늘날의 스마트폰 사용자들은 고속의 이동통신망을 기반으로 하는 다수의 모바일 서비스들을 사용하고 있다. 스마트폰이 제공하는 다양한 모바일 서비스들은 고속의 이동통신 네트워크 인프라를 요구하고 있으며, 이로 인하여 국내 이동통신 시장은 3G WCDMA 망에서 4G LTE 망으로의 급격한 전환이 이루어졌다. '13년 6월을 기점으로 4G LTE 망 가입자 수는 3G WCDMA 망 가입자 수를 넘어섰으며, 월 평균 100만 가입자 이상의 지속적인 증가세를 나타내고 있다.[1]

반면, LTE 망 사용자에 대한 보안 기술의 발전 속도는 가입자 증가 속도를 따라가지 못하고 있다. 이는 기존 이동통신망이 가진 폐쇄적 서비스 구조 특성상 망 내부에 적용되는 보안 장비 및 보안 정책에 대한 연구의 필요성이 인지되지 못했기 때문이다. 따라서 이동통신망의 특성을 반영한 다양한 보안 취약점에 대비하는 기술 개발이 시급히 요구된다.

모바일 망은 한정된 무선 자원을 가지고 있으며, 이를 효율적으로 관리하기 위하여 일정 시간 동안 사용이 없는 단말의 무선 자원을 해제하고, 다시 데이터를 송수신할 때 무선 자원을 재할당한다. 이 과정에서 무선 자원의 설정을 위해서 망 장비 간 다수의 시그널링 메시지들이 전달되게 된다. 따라서 악의적인 단말이 반복적인 무선 자원 할당/해제를 통한 대량의 시그널링 메시지를 유발시킴으로써 무선 자원을 관리하는 모바일 망 장비의 장애를 유발하는 공격을 시도할 수 있는데, 이를 시그널링 DoS라고 한다[2].

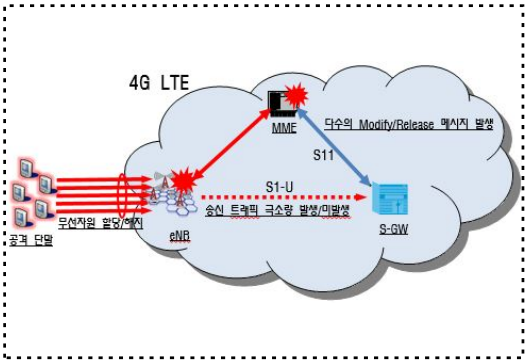

그림 1. 4G LTE 망에서의 시그널링 DoS

3G WCDMA 망의 경우 데이터 통신 경로와 시그널링 메시지 통신 경로가 동일하기 때문에, 망 장비 증설을 통하여 시그널링 DoS에 대한 위협을 감소시킬 수 있다. 하지만 4G LTE 망의 경우 그림 1에서와 같이 데이터 통신 경로와 시그널링 메시지 통신 경로가 분리되어 있기 때문에, 데이터 트래픽 량 증가에 대응하여 데이터 통신 대역폭만을 증가시킬 경우 시그널링 DoS에 대한 위협을 감소시킬 수 없다. 따라서 공격자가 상대적으로 대역폭이 좁은 시그널링 메시지 경로를 노려서 시그널링 DoS 공격을 시도하는 경우, eNodeB, MME 등의 제어 메시지를 처리하는 망 장비에 장애를 유발시킬 것으로 우려된다.

본 논문에서는 4G LTE 망에서 반복적인 망 연결/해지를 통하여 장애를 유발하는 시그널링 DoS 트래픽을 탐지하기 위한 기술을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 4G LTE 망에서 시그널링 DoS 공격 탐지를 위하여 진행되어온 관련 연구를 설명하고, 3장에서 제안하는 시그널링 DoS 공격 탐지 기술을 제시하며, 4장에서는 결론 및 향후 연구 방향에 대하여 기술한다.

Ⅱ. 관련 연구

최근 이동통신망에서 발생 가능한 여러 보안 위협들에 대응하기 위하여 다양한 기술들이 연구되고 있다. Ricciato가 3G WCDMA 망에서의 DoS 공격 모델에 대하여 소개한 [4]의 경우, Paging, DCH(Dedicated Channel) 할당 등 DoS 공격을 위한 여러 모델들을 소개하고 있으나, 이를 탐지하기 위한 구체적인 알고리즘은 소개하고 있지 않다. Patrick은 [2]에서 3G 망에서의 시그널링 DoS에 대한 주제를 제시하였다. 해당 논문에서는 반복적인 무선 연결/해지를 탐지하기 위한 알고리즘을 제시하였으나, 이는 3G 망을 기반으로 한 것으로 4G LTE 망을 대상으로는 적용이 불가능하다. Bassil은 [3]에서 4G LTE망에서의 시그널링 DoS에 대하여 소개하면서, 공격 방법으로 다수의 Dedicated Radio Bearer를 반복적으로 할당/해지하는 시나리오를 제시하고 있다. 그러나 LTE 망에서 Dedicated Bearer를 할당하려면 망 장비인 PCRF가 베어러의 할당을 요청해야 하는데, Bassil은 PCRF에 베어러 할당을 유발시키는 방법을 소개하지 않고 있으므로 이 방법을 이용한 공격은 현실성이 낮다.

본 논문에서는 단말이 활성(Active) - 휴지(Idle) 상태 전환을 이용하여 망에 무선 자원의 반복적인 설정을 유발하는 시그널링 DoS 공격방식에 대하여 논한다.

Ⅲ. 시그널링 DoS 탐지 알고리즘

4G LTE 망에서서 시그널링 DoS를 탐지하기 위한 알고리즘은 그림 2와 같이 제어메시지 분석을 통한 단말 별 무선 자원 할당 및 해지를 탐지하는 단계와, 무선 자원 할당 및 해지 기간 동안 송수신 트래픽 분석을 통한 비정상적 무선자원 할당을 탐지하는 단계, 그리고 비정상적 무선 자원 할당의 주기를 분석하여 시그널링 DoS 공격 여부를 판정하는 세 단계를 거치게 된다.

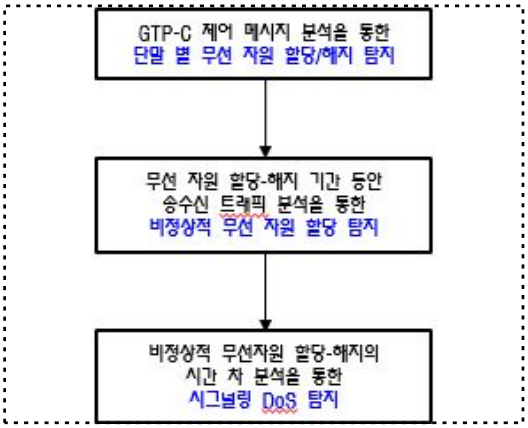

그림 2. 시그널링 DoS 탐지 알고리즘

3.1 단말별 무선 자원 할당/해지 탐지

4G LTE 망에서는 단말에 무선 자원이 할당되는 경우는 크게 세 가지 경우로 분류된다. 초기 Attach를 통한 할당의 경우와 핸드오버(Handover)를 통한 할당, 휴지 상태에서 활성 상태로의 전환을 통한 할당의 경우로, 세 경우 모두 MME와 S-GW 사이의 구간인 S11 구간에서 Modify Bearer Request, Modify Bearer Response 메시지를 주고받는다. S11 구간에서 이 메시지 쌍을 확인한다면, 해당 단말의 무선 자원에 대한 할당이 이루어졌음을 탐지할 수 있다.

무선 자원이 해지되는 경우 역시 세 가지 경우로 분류가 가능한데, Detach를 통한 해지, 핸드오버를 통한 다른 eNB 구간으로의 전환을 통한 해지, 활성 상태에서 휴지 상태로의 전환을 통한 해지의 경우로 나눌 수 있다. 이 가운데 Detach를 통한 해지의 경우에는 활성-휴지 상태 전환을 통한 공격보다 재연결까지 더 많은 시간이 소요되므로 시그널링 DoS의 공격방법으로 효과적이지 않으며, 핸드오버의 경우 역시 비정상적인 무선 자원 할당으로의 조작이 어려우므로 본 논문의 고려대상에서 제외한다. 상태 전환을 통한 무선 자원 연결의 경우, 연결이 해지되는 시점에서 S11 구간을 모니터링하면 Release Access Bearer Request, Release Access Bearer Response 메시지를 주고받는 것을 알 수 있다. 따라서 S11 구간에서 이 메시지 쌍을 확인한다면, 해당 단말의 무선 자원에 대한 해지가 이루어졌음을 탐지할 수 있다.

3.2 비정상적 무선 자원 할당 탐지

Modify Bearer Request와 Modify Bearer Response 메시지를 통한 연결이 정상임을 확인하기 위해서는, 해당 연결시각에서 해지시각까지 생성된 데이터 베어러를 통하여 데이터 트래픽이 정상적으로 발생하는지를 확인한다. 다수의 시그널링 메시지를 발생시켜서 망에 부하를 주는 연결은 반복적인 연결을 위하여 망에 전송하는 데이터 트래픽이 없거나 극소량 발생하는 특징을 가진다. 따라서 eNB와 S-GW 사이의 구간인 S11 구간의 트래픽을 모니터링하여, 특정 연결 시간동안 해당 단말이 송신하는 트래픽을 확인한다면, 해당 연결이 정상인지 비정상인지를 판별이 가능하다.

특정 패킷에서 송신한 단말을 식별하기 위해서는 이전 단계에서 관찰된 Modify Bearer Request와 Modify Bearer Response 메시지를 확인한다. 망 장비들은 각 단말의 데이터를 구분하기 위하여 TEID(Tunnel Endpoint Identifier)를 식별자로 사용하는데, Modify Bearer Request 메시지에는 S1-U 구간에서 eNB가 사용할 TEID 정보가 들어가며, Modify Bearer Response 메시지에는 S1-U 구간에서 S-GW가 사용할 TEID 정보가 들어간다. 따라서, 이 정보를 미리 데이터베이스화하여 관리한다면, 해당 TEID를 사용하는 데이터 패킷이 어떤 단말인지를 식별할 수 있다.

3.3 시그널링 DoS 탐지

특정 단말에 대한 비정상적인 무선 자원 할당 정보를 누적하여 관리하면, 얼마나 반복적이고 주기적으로 비정상적인 무선 자원 할당이 발생하였는지에 대한 분석이 가능하다. 시그널링 DoS 탐지는 그림 3과 같이 비정상적인 무선 자원 할당에 대한 스코어를 각 단말별로 누적 계산하여, 그 값이 임계값 k 이상이 될 경우 시그널링 DoS로 탐지하도록 한다.

$$S_i = \max\{S_{i-1} + (\frac{-T}{\alpha} + 1),\ 0\} \quad (1)$$

위 수식에서, S는 스코어, i는 현재 측정시점, i-1은 이전 측정시점이며, T는 비정상적 무선 할당이 발생한 시간의 간격이고, α는 T가 정상적인 시간간격을 가질 경우 $T < \alpha$, 비정상적인 시간간격을 가질 경우 $T \geq \alpha$가 되도록 설정하는 변수이다. 그림 3에서, T_2를 합산하는 경우 정상적인 시간간격을 가져서 누적값 S_i가 감소한 경우를 나타낸다.

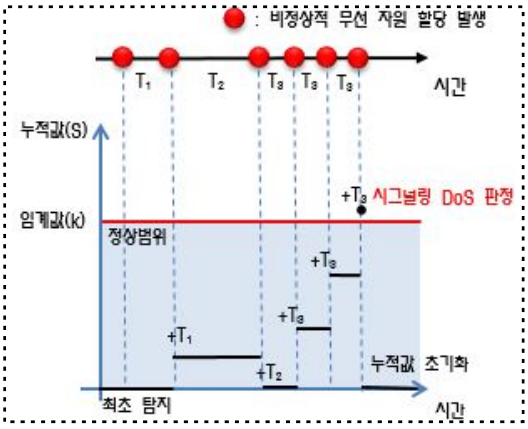

그림 3. 시그널링 DoS 탐지 방법

Ⅳ. 결론 및 향후 연구방향

본 논문에서는 단말별 무선 자원 할당/해지를 탐지하고, 송수신 트래픽 분석을 통한 비정상적인 무선 자원 할당을 탐지하며, 이를 통하여 4G LTE 망에서의 시그널링 DoS 공격을 탐지할 수 있는 기술을 제안하였다. 제안한 기술은 구현 및 성능/기능 검증을 통하여 국내의 상용 이동통신망에서 보안 위협을 대응하는 용도로 사용할 수 있으며, 기 구현된 이동통신망 관리 시스템에 모듈 형태로 추가 구현하는 방법으로도 활용이 가능하다. 단, 현재는 상용망에 대한 충분한 검증이 이루어지지 못한 단계이므로 향후 해당 알고리즘의 구현을 통한 검증 및 고도화 연구를 수행할 예정이다.

ACKNOWLEDGEMENT

본 연구는 미래부가 지원한 2013년 정보통신·방송(ICT) 연구개발사업의 연구결과로 수행되었음.

참고문헌

[1] 미래창조과학부, “유무선통계(2013. 7)”, http://www.msip.go.kr/www/brd/m_220/view.do?seq=385

[2] P. LEE, T. Bu, T, Woo, “On the Detection of Signaling DoS Attacks on 3G Wireless Networks”, Proceeding of InfoCom 2007, May 2007.

[3] R. Bassil, A. Chehab, I. H. Elhajj, A. Kayssi, “Signaling Oriented Denial of Service on LTE Networks”, Proceeding of MobiWac 2012

[4] F. Ricciato, “A review of DoS attack models for 3G cellular networks from a system-design perspective”, ACM Computer Commun,, Vol. 33, 2010