LTE 에서의 암호화된 트래픽 모니터링을 통한 비디오 서비스 식별 공격

손민철 [1], 배상욱 [1], 김동관 [1], 이지호 [2], 박철준 [1], 오범석 [1], 손수엘 [2], 김용대 [1]

KAIST [1] 전기및전자공학부, [2] 정보보호대학원

{mcson, hoops, dkay, jiholee, fermioncj, beomseoko, sooel.son, yongdaek}@kaist.ac.kr

Video Service Identification Attack in LTE by Monitoring Encrypted Traffic

Mincheol Son[1], Sangwook Bae[1], Dongkwan Kim[1], Jiho Lee[2], CheolJun Park[1],
BeomSeok Oh[1], Sooel Son[2], Yongdae Kim[1]
[1]School of Electrical Engineering, [2]Graduate School of Information Security, KAIST

요 약

본 논문에서는 기지국이나 단말의 접근 권한이 없는 공격자가 기지국으로부터 방송되는 정보만을 사용하여, 기지국내의 사용자가 어떠한 동영상 스트리밍 서비스를 사용하는지 식별하는 공격을 소개한다. 본 공격에서는 기지국이 각 단말마다 할당된 하향링크 자원 및 모듈레이션/코딩 정보를 사용하여 공격자가 단말별 하향링크 데이터 양을 유추 가능하며, 동영상 스트리밍 서비스마다의 동작 설정 차이로 발생되는 트래픽 모양의 특징적인 차이를 바탕으로 결정트리 분류 기법을 활용하여 공격자가 대상 기지국 내의 사용자들이 사용중인 동영상 서비스를 식별 가능함을 보여준다.

Ⅰ. 서 론

이동통신망 기술의 발달로 모바일 장치에서 비디오 스트리밍 서비스 사용은 점차 증가하여 2022 년에는 모바일 데이터 사용량의 80%를 차지할 것으로 예상된다[1]. 그 중, 현재 많은 사용자들이 사용하고 있는 동영상 스트리밍 서비스로는 넷플릭스(Netflix), 유튜브(YouTube), 아마존(Amazon Prime) 등이 존재한다. 이러한 스트리밍 서비스 사업자들은 하나의 동영상이 여러 개의 조각(chunk)으로 나뉘어 단말에게 순차적으로 전송하는 HTTP Adaptive streaming(HAS) 동영상 전송 방식을 사용한다.

LTE 를 통한 단말로의 동영상 전송 과정은 두 단계의 암호화 과정이 적용된다. 먼저, 동영상 스트리밍 서비스가 단말에게 동영상을 전달하는 과정에서 HTTPS 가 적용되어 동영상 스트리밍 데이터는 암호화되어 전달된다. 이후, 데이터가 LTE 망을 통하여 단말에게 전송되는 과정 중, LTE 무선 구간에서는 기지국이 단말과 설정된 키를 기반으로 데이터를 암호화하여 전송한다.

본 논문에서는 이러한 노력에도 불구하고, 공격자가 기지국이나 단말의 접근 권한 없이, Software-defined radio(SDR) 장비만을 사용하여 기지국이 방송하고 있는 정보, 즉 기지국 내에 존재하는 단말들로의 하향 링크 데이터 트래픽이 수집 가능하다는 것을 보여준다. 또한 동영상 스트리밍 서비스 별로 서로 다른 HAS 동작설정이 트래픽 모양에 끼치는 영향을 분석함으로써, 공격자가 암호화되어 전달되고 있는 트래픽만을 모니터링하여 각 단말이 어느 동영상 서비스를 사용하고 있는지 식별 가능하다는 것을 보여준다.

Ⅱ. LTE 기지국에서의 하향 데이터 전송 및 취약점

LTE 기지국(eNodeB)은 각기 다른 목적의 여러 채널을 통해 데이터를 전송한다. 그 중 사용자 데이터와 밀접한 연관이 있는 채널은 PDCCH(Physical Downlink Control Channel)과 PDSCH(Physical Downlink Shared Channel)로, PDCCH 는 사용자 데이터 획득을 위한 제어 정보(DCI: Downlink Control Information)를 제공하며 PDSCH 는 실질적인 사용자 데이터를 제공한다. DCI 는 1) 데이터가 할당된 무선 프레임 상의 리소스 블록(즉, 단말이 데이터를 검색해야 하는 주파수와 타이밍 정보), 2) 할당된 블록을 디코딩하기 위한 변조 코딩 방식(MCS), 3) 단말의 임시 식별자(RNTI)로 마스킹된 CRC 비트를 포함하며 매 LTE 서브 프레임(1ms)마다 전송된다. 단말은 기지국이 전송하는 DCI 정보를 확인하여, 자신에게 할당된 리소스 블록을 확인하고 PDSCH 로 전송되는 데이터를 MCS 정보를 활용하여 획득한다. 이후 기지국과 공유된 암호키를 사용하여 복호화한다.

(취약점) DCI 가 전송되는 PDCCH 는 암호화되지 않는 채널이므로 기지국의 모든 사용자의 DCI 는 노출되어 있다. PDSCH 상의 실제 사용자 데이터는 암호화되어 있지만, 데이터 전송 용량과 같은 정보는 암호화되어 있지 않다. 따라서 공격자는 PDCCH 내에 있는 모든 DCI 를 모니터링하여 기지국내 존재하는 단말들의 DCI 정보를 취득하고, 각 단말 별로 하향 데이터 사용량을 알아 낼 수 있다[2,3]. 이러한 모니터링 과정은 SDR 을 사용하여 수행 가능하며, 본 연구에서는 PDCCH 를 디코딩하고 각 RNTI 별로 할당된 데이터양을 분석하는 장비인 AirScope[4]를 사용하였다.

Ⅲ. 동영상 서비스 별 동작 분석 및 결정트리 생성

가. 동영상 스트리밍 트래픽 수집

비디오 트래픽을 수집하기 위해 실제 공격 상황과 같도록 환경을 설정하였다. 상용 단말을 이용해서 비디오를 재생시키고, 무선 신호 캡쳐 장비를 사용하여 해당 단말에게 전송하는 무선 신호 트래픽을 수집하였다. 데이터 수집을 위해 사용한 단말은 갤럭시 노트 5 와 갤럭시 S6 Edge 이며, 한국의 세 통신사에 대해 모두 데이터 수집을 진행하였다. 본 연구에서는 유튜브, 넷플릭스, 아마존 서비스를 대상으로, 각 서비스에 대해 비디오를 선정한 후 한 비디오에 대해 여러 번 반복하여 데이터를 수집하였다. 사용한 비디오 서비스 및 비디오 수는 표 1 과 같다. 하나의 비디오 트래픽 수집을 위해 비디오는 0 초부터 120 초까지 재생하였다.

표 1 비디오 트래픽 데이터

서비스	비디오 종류 (개)	비디오 트래픽 수 (개)
YouTube	30	847
Netflix	22	845
Amazon	27	873

나. 동영상 서비스 별 동작 분석 결정트리 생성

우선 결정트리를 설계하기에 앞서 비디오 서비스에 따라 트래픽의 모양이 어떻게 차이가 나는지 분석을 진행하였다. 그림 1 은 유튜브와 아마존에서 비디오 트래픽의 개형을 보여준다. 가장 큰 차이는 비디오가 처음 시작하는 부분에서 데이터를 받는 양과 시간이다. 유튜브는 1~2 초 간격으로 단말에 데이터를 전송하지만 아마존은 첫 6 초간 지속적으로 데이터를 전송한다. 또 다른 차이는 연속된 두 chunk 사이의 간격이다. 유튜브와 아마존의 경우는 평균 4 초 정도로 chunk 의 간격이 비슷한 반면 넷플릭스에서는 약 44 초의 큰 값을 가지는 것을 확인하였다.

이러한 비디오 서비스에 따른 트래픽 개형의 특징은 서비스 제공자의 HAS 설정에 따라 나타나는 현상이다. 본 연구에서는 비디오 서비스 제공자를 분류하기 위해 트래픽의 특징을 반영하는 결정트리를 설계하였다. 그 결과 비디오 서비스 결정트리에 사용된 feature 는 총 6 가지이다. 120 초 동안의 chunk 개수, 처음 데이터를 다운로드 받는 시간, 첫 데이터를 받은 후 다음 데이터를 받기까지의 시간, chunk 사이의 시간 간격 정보(평균, 최소, 최대)가 사용되었다. 이러한 feature 들은 서비스 사업자들의 설정(첫 초기 재생 버퍼의 길이, chunk 의 길이, HAS 알고리즘에 따른 chunk 요청 주기)을 반영하여 서비스에 따라 다르게 나타난다.

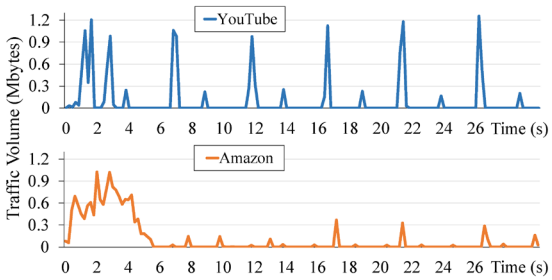

그림 1 YouTube 와 Amazon 무선 트래픽

다. 실험 결과

앞서 설명한 feature 를 가지고 실제 비디오 서비스 결정트리를 생성하여 해당 서비스를 식별할 수 있는지 확인하였다. 결정트리를 생성하기 위해 Python sklearn 모듈에 포함된 DecisionTreeClassifier 를 이용하였다. 생성된 결정트리가 학습에 사용되지 않은 비디오에 대해서도 높은 성능을 보이는지 확인하기 위해 수집된 데이터를 나누어 실험하였다.

결정트리 학습을 위해서는 유튜브, 넷플릭스, 아마존에 대해 각각 23, 17, 20 개의 비디오 데이터인 617, 620, 623 개의 트래픽을 사용하였다. 그 외 나머지 데이터는 완성된 결정트리의 알 수 없는 비디오에 대한 성능 검증을 위해 사용되었다.

실험결과 학습된 결정트리는 그림 2 와 같으며, 실험에 사용되지 않은 알 수 없는 비디오에 대해서는 각각 유튜브(0.97), 넷플릭스(1.00), 아마존(0.98)의 정확도를 보였다. 이는 결정트리를 생성하기 위해 사용되는 비디오가 아닌 전혀 모르는 비디오 트래픽에 대해서도 비디오 서비스를 식별할 수 있음을 의미한다.

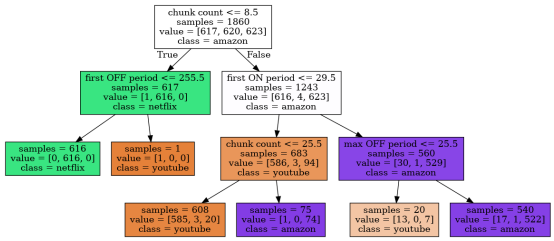

그림 2 비디오 서비스 결정트리

비디오 서비스 결정트리는 각 비디오 서비스를 분류함에 있어서 두 가지 특징이 주로 사용된다. 첫 번째로 그림 2 에서 볼 수 있듯이 넷플릭스와 다른 비디오 서비스는 chunk 개수에 따라 분류된다. 이는 위에서 언급했듯이 chunk 간의 간격이 넷플릭스가 훨씬 길기 때문에 같은 120 초 트래픽에서의 chunk 개수가 다른 비디오 서비스에 비해 작은 값을 가진다.

두 번째로, 유튜브와 아마존은 처음 데이터를 받는 시간에 따라 분류된다. 그림 1 에서와 같이 유튜브는 어느 정도 규칙적인 데이터 양을 전송하는 것에 반해 아마존은 처음 수신하는 데이터 양이 확연히 많다. 이러한 특징에 의해 비디오 트래픽의 서비스 제공자를 식별할 수 있다.

따라서 공격자는 각 비디오 서비스에 대한 트래픽을 가지고 있다면, 비디오 서비스 결정트리를 생성할 수 있고 이를 이용하여 LTE 사용자들이 어떤 비디오 서비스를 이용하고 있는지 손쉽게 알 수 있다.

Ⅲ. 결론

본 논문에서는 기지국이나 대상 단말에 대해 아무런 접근권한이 없는 공격자가 기지국 서비스 범위내의 사용자들이 어떠한 동영상 서비스를 사용하고 있는지 식별하는 공격이 가능함을 논의하였다. 향후 연구에서는 이러한 트래픽 모양을 기반으로 동영상의 제목 등 사용자의 프라이버시를 침해하는 추가적인 공격의 가능성을 분석하고자 한다.

ACKNOWLEDGMENT

이 논문은 2021 년도 정부 (과학기술정보통신부)의 재원으로 정보 통신기획평가원의 지원을 받아 수행된 연구임 (No. 2018-0-00831, 이종 무선 네트워크를 위한 물리 계층 보안 기술 연구).

참 고 문 헌

[1] Sandvine, 2019. Mobile Internet Phenomena Report https: //www.sandvine.com/2019-mobile-internet-phenomena-report.

[2] Kohls, K., Rupprecht, D., Holz, T. and Pöpper, C., 2019, Lost traffic encryption: fingerprinting LTE/4G traffic on layer two. In Proceedings of the Conference on Security and Privacy in Wireless and Mobile Networks (WiSec).

[3] Balasingam, A., Bansal, M., Misra, R., Tandra, R., Schulman, A. and Katti, S., 2017, October. Poster: Broadcast LTE data reveals application type. In Proceedings of the International Conference on Mobile Computing and Networking.

[4] srsLTE, AirScope, http://www.softwareradiosystems.com/tag/airscope.