BT-uTP 프로토콜 동작 방식에 관한 연구

이세린, 김명수, 배주혁, 오태규, 라도훈, 최원영, 이경문*
아주대학교, 극동대학교, 한양대학교, 동의대학교, 울산제일고등학교, 경찰대학교, *중부대학교
serinee95@gmail.com, sec1319@naver.com, bjh512512@gmail.com,
ohseoh44@gmail.com, citron0137@gmail.com, fl0ckfl0ck@hotmail.com, *gilgil1973@gmail.com

A Study on operation methods of BT-uTP protocol

Lee Se Rin, Kim Myoung Soo, Bae Ju Hyeok, Oh Tae Gue, Ra Do Hoon, Choi Won Young Lee Kyoung Moon*
Ajou Univ., Far East Univ., Hanyang Univ., Dong-Eui Univ., Ulsan Jeil High school, Korea National Police Univ., *Joongbu Univ.

요 약

BitTorrent 파일전송 프로토콜 중 하나인 BT-uTP 프로토콜은 더욱 신속한 전송을 위해 UDP를 활용하면서도 응용 계층에서 과부하 제어를 가능케 하여, 최근 대부분의 토렌트 어플리케이션이 BT-uTP를 전송 방식으로 채택하고 있다. 따라서 그 높은 사용률을 고려하였을 때 BT-uTP는 매우 중요한 프로토콜이다. 그러나 기존의 분석방법으로는 해당 프로토콜을 분석하는 데 한계가 있어 BT-uTP 프로토콜의 구조와 특성을 반영한 새로운 분석방법을 제시한다.

Ⅰ. 서 론

기존 Client-Server 방식의 한계를 극복하기 위해 도입된 P2P 프로토콜은 BitTorrent 프로토콜의 등장과 함께 사용량이 급증하였다. P2P 프로토콜은 사용자 수가 방대해지더라도 특정 단말에 부하가 집중되지 않기 때문에 확장성이 높고 Client-Server 방식보다 요구되는 서버의 사양이 낮다. 그러나 음란물, 저작물 배포 등 불법적인 행위에 P2P 프로토콜이 악용되고 있는 것이 사실이다.

그러나 이러한 P2P 프로토콜의 효용성은 일부 악용되어, 현재까지도 BitTorrent 프로토콜이 불법 음란물, 저작권으로 보호되는 콘텐츠들을 소유하고 배포하는 불법적인 행위에 지속적으로 사용되고 있다[1]. 물론 2010년 중반 이후, 실시간 스트리밍 프로토콜 (이하 RTSP)의 사용으로 인해 BitTorrent를 포함한 P2P 프로토콜의 사용량이 줄어들고 있는 것은 사실이다[2]. 그러나 RTSP 또한 과부하방지, P2P 기반의 효율적인 스트리밍을 위하여 BitTorrent 프로토콜을 기반 기술로 삼고 있다. 더불어, 2018년 7월 트론(Tron) 재단이 BitTorrent를 인수함으로써 암호화폐에서의 활용 가능성이 대두되는 만큼 비트토렌트 프로토콜의 분석에 대한 지속적인 연구가 필요하다[3].

BT-uTP 프로토콜은 어플리케이션 레벨의 과부하를 제어하고 속도가 향상된 형태의 비트토렌트의 프로토콜로 분석대상으로서의 가치가 매우 높으나 기존의 분석방법으로는 헤더 이외에 세부적인 분석에 애로사항이 있다. 그래서 본 논문에서는 비트토렌트 프로토콜 중 BT-uTP 프로토콜의 구조를 살펴보고 개선된 분석방법론을 제시하고자 한다.

Ⅱ. 본론

Ⅱ-1. BitTorrent 프로토콜 개요

BitTorrent 프로토콜의 근본 원칙은 "공정함"이라고 할 수 있다. 개발자 Bram Cohen이 모델로서 사용한 Tit-For-Tat Game 방식은 생물학에서의 '상호이타성'과 비슷한 개념으로 BitTorrent 프로토콜의 최대 장점인 Peer Picking의 기본이 된다[4]. 근래에 들어서 BitTorrent는 Tracker를 적극적으로 활용하는 등 Peer Picking 방식이 다양해지고 있지만, 가장 우선시하는 원칙은 '자신에게 유리한 Peer'에게 먼저 업로드한다는 원칙이다. 즉, 다른 Peer들에게 업로드는 하지 않고 다운로드만 받는 Leecher에게는 자신이 가진 Piece를 잘 주려고 하지 않는다. 즉, 가능한 많은 Peer들에게 업로드하는 것이 자신에게나 다른 Peer들에게나 유리한 방식으로 동작한다는 것이다[5]. 실제로, 아무런 활동을 하지 않는 두 PC가 어떠한 파일을 배포하고 배포 받으려 한다면, 다운로드에 상당히 오랜 시간이 걸린다.

BitTorrent 프로토콜이 Peer를 선택한 후 데이터를 주고받는 방식은 Wireshark와 같은 패킷 분석 도구를 이용하여 분석할 수 있다. BitTorrent는 자신만의 독특한 인코딩 방식을 사용하는데, 이를 Bencoding이라고 한다. Bencoding은 토렌트 파일을 다운로드 받기 위해 필요한 .torrent 파일에 사용된다. 또한, 실제 데이터 교환을 시작하면서 각종 메타데이터를 전송할 때에도 사용한다. 즉, BitTorrent 프로토콜을 통해 실제 Payload를 전송하는 과정에서 사용되는 BitTorrent 메시지 분석 뿐만 아니라, Bencoding된 메시지를 Bdecoding하여 메타데이터를 분석하는 과정도 중요하다. 이어서 Payload를 전송하기 위해 사용되는 BitTorrent 메시지로는 총 10종류가 존재하는데, 각 메시지는 고유의 ID(range 0-9)를 가지고 있다.

먼저, 9라는 ID를 가지는 Port 메시지는 Peer가 자신이 어떤 Port로 BitTorrent 통신을 할 것인지를 Seeder에게 알린다. 여기서 주의할 점은, 우리가 4계층인 전송 계층(Transport Layer)에서 전송하는 Port 번호와는 다르게, Raw Packet 속 2 바이트를 10진수로 해석하는 것이 아닌 2 바이트를 그대로 10진수로 읽어 내야 한다는 것이다. 다음으로 1과 2라는 ID에 해당하는 Unchoke와 Interested Message이다. 이 두 Message는 업로더와 다운로더가 서로 연결을 수립할 때 보이는 메시지로서, 다운로더는 업로더의 Piece를 원한다는 의미에서 Interested Message를 보내고, 업로더는 다운로더에게 업로드 해주겠다는 '선택'의 의미로 Unchoke Message를 전송한다. 반대로, 0과 3이라는 ID에 해당하는 Choke, Not Interested -Message는 연결을 해제할 때 보이는 메시지로서 해석하면 된다. 마지막으로 4, 5, 6, 7, 8에 해당하는 ID는 업로더와 다운로더의 Piece 선택과 전송에서 사용되는 실질적 데이터 교환과 밀접한 메시지로, 다음에 말할 BT-uTP에서 좀 더 면밀히 분석할 예정이다.

Ⅱ-2. BT-uTP 프로토콜 분석

BT-uTP는 BitTorrent 프로토콜이 TCP 위에서 동작하는 것과 달리, UDP 위에서 동작하는 변형된 형태의 BitTorrent 프로토콜이다. 이는 uTorrent에서 개발한 프로토콜인데, UDP를 통한 패킷 전송이 TCP를 통한 패킷 전송보다 더 빠르다는 관점에서 가치가 높다. UDP를 통해 전송할 시 발생할 수 있는 Packet Loss는 BT-uTP가 방지한다. 이것이 가능한 이유는 BT-uTP 프로토콜은 기존의 UDP Header에서 Reliable Transport를 지원하기 때문이다. 높은 안정성과 더불어 속도향상으로 BitTorrent는 BT-uTP를 정식 채택하여 많은 양을 이를 통해 전송하도록 지원하고 있다. BT-uTP는 BitTorrent 프로토콜과 전송 방식에서 차이가 난다. BitTorrent 프로토콜은 Header가 없지만, BT-uTP는 Header를 가지고 있으며 시더와 연결을 맺는 방식이 다르다. 실제로, Reliable Transport를 하기 위해 BT-uTP는 그 TYPE으로서 Data(0), Fin(1), State(2), Reset(3), 그리고 Syn(4)을 가진다. 즉, Syn으로 연결을 맺고, Fin으로 연결을 끊는다.

한편, 두 프로토콜의 데이터 교환 방식에서는 비슷한 구조를 가진다. 두 프로토콜이 사용하는 데이터 교환 방식은 패킷 내 Message를 활용하는 것인데, BT-uTP는 위에서 설명한 BitTorrent Message와 동일한 유형의 Message를 지원한다. BitTorrent Message ID가 5 에 해당하는 Bitfield는 Peer들이 연결을 맺자마자 다른 어떠한 데이터를 주고 받기 전에 자신이 갖고 있지 않은 Missing Piece에 대한 정보를 0(Missing), 1(Existing)로 표현해 전송한다. 이는 필수적인 것은 아니나, Peer 간 앞으로 전송할 Piece 선택에 영향을 줄 것으로 생각된다. 다음으로 ID가 4인 Have, Piece와 ID가 6인 Request, Piece는 Peer 중 다운로더가 보내는 메시지로, 전자는 자신이 가진 Piece가 어떤 것인지 알림으로써 중복된 Piece를 받는 것을 방지해 부하를 줄이도록 하고, 후자는 자신이 받길 원하는 Piece를 요청하여 업로더가 전송하도록 한다. 마찬가지로 ID가 8일 때 역시 다운로더가 여러 Peer들에게 같은 Request, Piece를 보낸 후 가장 먼저 업로드 해줄 수 있는 Peer로부터 Piece를 받으면 나머지 Peer들에게 취소 메시지로서 Cancel, Piece를 보내게 된다. 이와 같은 메시지는 BitTorrent의 특징으로서 빠르고, 중복을 최소화하는 데이터 교환 방식이라고 볼 수 있다. 반면 업로드를 수행하는 Peer들은 다운로드하는 Peer에게 ID가 7인 Piece Message를 전송하는데, 이것은 Request, Piece에 대한 응답과 같이 동작한다. 즉, 요청받은 Piece에 대한 실제 데이터를 전송하는 패킷이다. 결론적으로 BitTorrent나 BT-uTP는 앞서 설명한 Piece message를 통해 데이터를 전송하고, 전송받도록 하며, 이러한 동일한 원리를 통해 같은 방식으로 BT-uTP 프로토콜을 분석할 수 있다.

우리는 현재, Wireshark Lua Plugin 제작을 통해 일차적인 프로토콜 분석이 Wireshark나 Tshark에서 가능하도록 제작하고 있으며, 동시에 BitTorrent가 악용되어 발생하는 범죄에 대한 솔루션 분석을 수행하고 있다.

Ⅲ. 결론

BitTorrent가 개발된 지 17년이라는 시간이 흘렀지만, 아직까지도 수많은 Peer들의 데이터 교환에 중요한 역할을 할 뿐만 아니라, 다른 프로토콜이나 암호화폐에 사용되는 등 높은 활용성으로 스스로의 가치를 증명하고 있다. BitTorrent 프로토콜은 앞으로도 4차 산업혁명 시대에 대두되는 사물인터넷에 활용되며 무궁무진하게 사용될 수 있을 것이다. 현재는 개인이나 회사가 비트토렌트를 사용하여 그들 소유의 라이선스가 있는 자료를 배포하는 사례가 늘고 있다. 이런 것처럼 BiTorrent를 활용한 긍정적인 기능이 있는 반면 불법 소프트웨어, 불법 영화와 같은 저작권 위반부터 아동음란물과 같은 불법 영상물을 유포와 같은 범죄에 악용하는 등 역기능도 존재한다.

BitTorrent가 개발된 지 17년이라는 시간이 흘렀지만, 아직까지도 개인이나 회사가 라이선스가 있는 자료를 배포하기 위하여 사용될 뿐만 아니라, 다른 프로토콜의 기반이 되거나 암호화폐 등에 사용되는 높은 활용성으로 스스로의 가치를 증명하고 있다. BitTorrent는 앞으로도 4차 산업혁명 시대의 각광받는 사물인터넷에 활용되는 등 무궁무진하게 사용될 수 있을 것이다. 하지만 이러한 긍정적인 측면이 있는 반면 불법적으로 유포되는 소프트웨어나, 영화와 같은 저작권 위반행위부터 아동음란물 유포행위까지 범죄에 악용되는 등 부정적인 측면도 존재한다.

따라서 우리는 다양하게 활용되거나 악용되는 BitTorrent 프로토콜에 대한 심층적 분석을 통해 BT-uTP 프로토콜의 특성을 반영한 분석방법을 솔루션(Plugin) 형태로 개발하여 적용하고자 한다.

ACKNOWLEDGMENT

본 논문은 *KITRI 차세대 보안리더 양성 프로그램(Best of the Best) 지원을 받아 작성하였다.

참 고 문 헌

[1] 조화제, 김대형, 이재우 : “아동·청소년 음란물 유포자 추적 방안에 관한 연구 -비트 토렌트에 대한 포렌식 중심으로” - 2014

[2] Sandvine : “Global Internet Phenomena Report” - 2013

[3] Smartereum : “TRON Acquired BitTorrent for USD$140 Million, Blockchain Injects New Energy into BitTorrent” https://smartereum.com/25737/tron-acquired-bittorrent-for-usd140-million-blockchain-injects-new-energy-into-bittorrent/ - 2018

[4] Bram Cohen : “TORRENTS AND TIT-FOR-TAT” - 2012

[5] bittorrent, http://bittorrent.org