NDN(Named Data Networking)의 PIT에 대한 DDoS 공격 방지 연구

정수림, 최형기
성균관대학교 소프트웨어대학
todrkr147@g.skku.edu, meosery@skku.edu

A Study on the Prevention of DDoS Attack on PITs in NDN(Named Data Networking)

Soo-Rim Jeong, Hyoung-Kee Choi
Dept. of Computer Engineering, Sungkyuankwan University

요 약

DDoS(Distributed Denial of Service) 공격은 현재의 인터넷 환경뿐만 아니라 NDN에서도 정상적인 서비스를 저해시키는 주요 문제이며 이에 관련된 다양한 연구들이 진행되고 있다. 본 논문에서는 DDoS 공격이 가해질 때 NDN 라우터의 PIT(Pending Interest Table) 가용성 저해로 인해 발생하는 문제 해결에 중점을 둔다. 이를 위한 방안으로 RED(Random Early Detection) 알고리즘을 기반으로 하는 기법을 적용하고, 시뮬레이션을 통한 측정 결과를 보여준다.

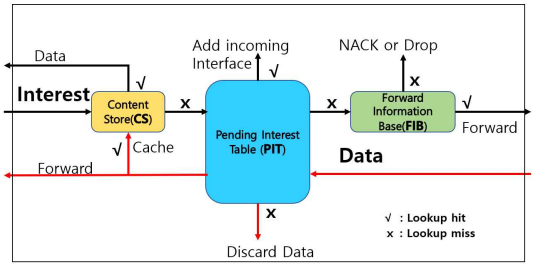
1. 서론

Named Data Networking(NDN)은 인터넷에서 콘텐츠 자체의 정보와 라우터 기능만을 이용하여 목적지로 데이터를 전송하기 때문에 TCP/IP 기반의 설계적인 제약점에 대한 해법을 제시한다. 그러나 오늘날에도 여전히 이루어지는 DDoS 공격에 대한 복원력은 새로운 아키텍처인 NDN에서도 주요 문제가 된다. 이를 위한 해결책으로 satisfaction-based Interest acceptance[1], Finegrained Interest Traffic Throttling(FITT)[2] 등이 있는데 각 알고리즘은 높은 확률로 interest 패킷을 조절할 수 있지만 요청자와 콘텐츠 제공자 사이에 홉 수가 증가함에 따라 확률이 저하된다는 단점이 있다. 따라서 본 논문에서는 홉 수의 영향이 없으면서 DDoS 공격 환경에서 정상 사용자의 Data 패킷 손실이 최소화될 수 있도록 하는 RED 알고리즘을 통한 해결방안 제시 및 시뮬레이션을 통한 측정 결과를 보여준다.

2. NDN 라우터 구성 및 동작 원리

NDN은 데이터 이름 기반의 요청 메시지(Interest)/ 응답 메시지(Data) 포워딩, 중간 네트워크 노드에서의 데이터 캐싱 및 포워딩, 전자 서명 기반의 데이터 인증과 같은 특징으로 요약될 수 있다[3]. 이러한 특징을 구현하기 위하여 NDN은 Forward Information Base(FIB), Pending Interest Table(PIT), Content Store(CS)를 사용한다. NDN 라우터는 Interest 패킷을 저장 후 PIT에 Interest 패킷의 이름과 패킷이 들어온 인터페이스 정보를 저장한다. Interest 패킷이 요청된 콘텐츠에 도달하면 Data 패킷에 콘텐츠를 수록하여 전송하게 되며, 이때 Data 패킷이 도착하면 PIT를 참조하여 Interest 패킷이 수신된 동일한 경로를 따라

역으로 전달된다. 이후 전달 된 패킷에 대한 라우팅 정보는 PIT 리스트에서 삭제되고, 전송된 콘텐츠는 Content Store에 저장된다. 만약 PIT에 저장되었던 Interest 정보가 없어진다면 Data 패킷이 라우터에 도착해도 전달 경로를 알 수 없기에 패킷은 삭제된다. (그림 1)은 NDN 구조에서 Interest와 Data 패킷 포워딩을 보여준다.



(그림 1) NDN 구조에서 Data 패킷 포워딩

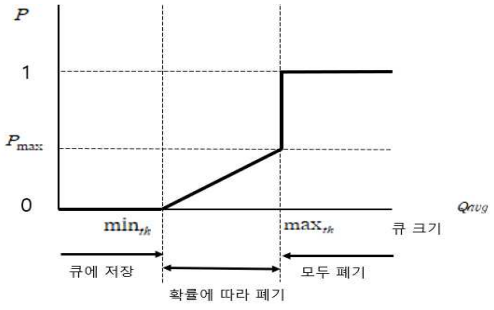
3. 관련 연구

NDN 환경에서 DDoS 공격을 완화하기 위한 방법에는 Satisfaction-based Interest acceptance, Finegrained Interest Traffic Throttling 기법 등이 있다. Satisfaction-based Interest acceptance 기법은 Interest satisfaction ratio를 들어오는 Interest를 받아들이거나 거절할 수 있는 직접적인 확률로 사용한다. Satisfaction-based Interest acceptance 방법의 단점은 경로상의 각 라우터가 Interest를 Forward 할지 또는 Nack(drop) 할지에 대해 독립적인 결정을 하므로 홉 수가 증가함에 따라 정당한 Interest가 전달될 확률은 급속히 감소하게 된다.

Finegrained Interest Traffic Throttling(FITT) 기법은 피해자가 NACK을 통해 현재 상태를 피드백하여 문제를 해결하는 방식이다. 공격자의 패킷이 최종 목적지인 피해자 서버까지 가면 서버는 전 단계 라우터에 FITT NACK으로 정보를 전달한다. 이후 라우터는 전달받은 정보를 바탕으로 해당 Interest가 온 경로인 Intereface를 통해 거꾸로 NACK을 전송한다. 매 라우터를 이런 과정을 통해 거친 후 최종적으로 Edge 라우터에서 최소 허용 트래픽 값을 계산하여 Interest 패킷의 전송률을 제한한다.

4. RED 알고리즘을 이용한 DDoS 공격 완화

RED 알고리즘은 EWMA(Exponentially Weighted Moving Average)를 이용하여 평균 큐 크기를 계산하고, 라우터의 큐의 길이가 일정한 값을 넘으면 확률에 의해 패킷을 폐기시키며 혼잡을 제어하는 방법이다. (그림 2)와 같이 패킷을 제어하기 위하여 큐의 길이에 대한 임계치로 두 개의 파라미터인 최소 임계값(**min**th)과 최대 임계 값(**max**th)을 가지는데, 평균 큐 길이(**avg**)가 최대 임계값보다 클 경우에는 모든 패킷을 폐기하고, 최소 임계값과 최대 임계값 사이에 있을 때는 폐기 확률(**P**max)에 의해 패킷을 확률적으로 폐기하며 최소 임계값보다 작을 경우에는 패킷을 큐에 저장한다.[4]



(그림 2) RED 알고리즘을 통한 패킷 폐기 확률

이러한 알고리즘을 통해 네트워크 혼잡이 발생하면 패킷을 선택적으로 삭제하여 DDoS 공격의 영향을 받는 라우터 가용성 저해를 최소로 유지한다. IP 네트워크 환경에서 RED 알고리즘은 IP를 우선순위로 가중치를 설정하여 효율을 더 높인다. 하지만

NDN 환경은 IP 네트워크 환경과 다른 구성을 가지고 있기때문에 특정 대상을 기준으로 가중치를 부여하지 않는 이상 알고리즘 자체만으로는 큰 효율이 나타나지는 않는다. 즉 공격자와 합법적인 사용자의 구분없이 Interest 패킷을 무작위로 삭제하면 적은 수로 보내지는 합법적인 사용자의 패킷이 삭제될 확률이 높아지게 된다. 따라서 DDoS 공격을 감지하고 대처하는 방법으로 일정 시간 기준으로 라우터에 대량으로 패킷(공격자의 Interest)이 들어오는 Interface를 구분하여 그 패킷들에 대해서만 RED를 적용하여 합법적인 사용자의 패킷이 삭제되는 것을 제한한다.

5. 시뮬레이션 측정 결과

측정을 위해 세팅해 놓은 시뮬레이션 환경에서 DDoS 공격과 비슷한 상황을 발생시키기 위해 공격자와 합법적인 사용자를 각각 2명씩 지정하였고 합법적인 사용자는 10 packets/sec, 공격자는 1,000 packets/sec으로 전송하도록 구현하였다. 측정 시간은 시뮬레이션 환경에서의 5초로 정도로 세팅하였다.

RED 관련 알고리즘 코드는 PIT에 Interest 패킷 이름 및 해당 패킷이 들어온 인터페이스 정보가 저장되는 Forwawrder.cpp의 IncomingInterest 함수에 추가하여 구현하였다. 공격자의 패킷으로 구별하는 방법은 주기적으로 일정 시간 동안 라우터의 각 인터페이스로 들어오는 Interest 패킷의 개수를 측정하고 이때 최대로 많은 패킷이 들어오는 인터페이스를 기준으로 정하였다.

<표 1>은 RED 알고리즘 적용 전과 후의 성능 비교 결과이다. 알고리즘 적용 전에는 NDN이 그 자체 설계만으로 이미 DDoS 공격을 효과적으로 제거할 수 있는 장점이 있음에도 측정 결과 합법적인 사용자가 받게 되는 Data 패킷 수는 Interest 패킷 수의 대략 60% 정도가 되는 것을 확인하였다. 알고리즘 적용 후에는 70% 이상 더 받는 것을 확인하게 되었다.

<표 1> RED 알고리즘 적용 전과 후 성능 비교

분류	Interest Packets	RED 적용 전	RED 적용 후	증가율 (%)
Attacker 1	2022	1195	1441	12.2
Attacker 2	2027	1184	1407	11.0
User 1	209	121	147	12.4
User 2	213	135	157	10.3

6. 결론

NDN 라우터에서 PIT는 소비자가 요청한 콘텐츠의 Data 패킷이 Interest 패킷의 경로를 따라 사용자에게 전송되도록 하는데 중요한 역할을 한다. 본 논문에서는 RED 알고리즘 기반의 새로운 기법을 제안하여 DDoS 공격이 발생할 때 PIT의 성능저하로 합법적인 사용자의 Interest 패킷이 삭제되는 현상이 일정 완화되는 것을 측정하였다. 이 알고리즘은 요청자와 인접한 라우터에서 적용되기에 라우터마다 결정할 과정을 거치지 않아 홉 수 증가에 따른 성능저하와 같은 부분을 보완할 수 있는 알고리즘이라고 할 수 있다.

ACKNOWLEDGEMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2020R1A2C1012708).

참고문헌

[1] Alexander Afanasyev, et al. "Interest flooding attack and countermeasures in Named Data Networking." 2013 IFIP Networking Conference Brooklyn NY USA May 2013 p.1-9.

[2] Zhang, Zhiyi, et al. "Expect more from the networking: DDoS mitigation by FITT in mamed data networking." arXiv preprint arXiv 1902.09033 Feb. 2019.

[3] Zhang Lixia, et al. "Named data

networking." ACM SIGCOMM Computer Communication Review 44.3 p.66-73 Jul. 2014.
[4] Floyd, Sally, and Van Jacobson. "Random early detection gateways for congestion avoidance." IEEE/ACM Transactions on networking 1.4 p.397-413 Aug 1993.