혼잡 회피 라우팅
반응형 BGP 라우팅을 통한 DDoS 공격과 불리한 네트워크 상황 극복

이 논문에서는 Nyx 시스템을 소개합니다. Nyx는 외부 협조나 인터넷 재설계 없이도 공격자가 조작하는 트래픽 양에 관계없이 현대적인 분산 서비스 거부(DDoS) 공격을 효과적으로 완화하는 최초의 시스템입니다. Nyx는 DDoS 완화를 필터링 문제가 아닌 라우팅 문제로 접근합니다. 이 개념적 전환은 Nyx가 기존의 학술 및 상업용 DDoS 완화 시스템의 많은 일반적인 결점을 피할 수 있도록 합니다. Nyx는 자치 시스템(Autonomous System, AS)이 존재하는 Border Gateway Protocol (BGP)에서 경로 광고를 처리하는 방식을 활용하여, 공격 대상 링크에서의 트래픽을 공격을 받는 상위 AS로부터 격리시키고 대안적인 혼잡하지 않은 경로로 유도합니다. 이 격리는 필터링이나 공격 트래픽의 우선순위 조정이 필요하지 않도록 합니다. Nyx는 외부 조정 없이 일반 BGP 경로 선택을 통해 출발 경로를 제어하고, 중요한 AS에서의 반환 경로는 우리가 개발한 특정 기술을 사용하여 트래픽 엔지니어링 원칙을 활용하며 외부 조정이 필요하지 않습니다. 우리만의 현실적인 인터넷 규모 시뮬레이터를 사용하여, 우리 시스템이 전송 링크 DDoS 공격에서 중요한 트래픽을 거의 98% 이상의 경우에 효과적으로 라우팅할 수 있는 것으로 확인했습니다. 이러한 공격은 공격 트래픽이 피해 AS에 도달하지 않으므로 방어적 필터링, 조절 또는 우선순위 지정 전략이 무용지물이 되는 새로운 형태의 DDoS 공격입니다. 더 중요한 것은 이러한 경우의 95% 이상에서 대체 경로가 전송 링크 DDoS로부터 완전한 혼잡 완화를 제공한다는 것입니다. 또한 Nyx는 직접 공격을 받는 경우에는 75% 이상의 경우에 완전한 혼잡 완화를 제공합니다.

I. 소개

분산 서비스 거부 (DDoS) 공격은 인터넷에서 가장 크고 해결되지 않은 위협 중 하나로 여겨지며 기술 복잡성이 낮은 반면 파괴적인 영향력을 가지고 있습니다. 최근 Mirai 봇넷에 의한 DDoS 공격은 루트 DNS 공급자 [1] 및 핵심 전송 링크 [2]에 성공적으로 수행되었으며 이는 DDoS 공격에 대한 효과적인 배치된 솔루션이 부재하고 있으며 이러한 공격이 중요한 네트워크 인프라에 미치는 영향을 강조합니다. 대역폭을 증가시켜 악의적인 적대자들이 하향 희생자가 필터링할 수 없을 만큼 엄청난 트래픽 흐름을 가지고 파괴적인 공격을 시작할 수 있게 한 봇넷들은 전략적인 적대자들에게 기회를 제공했습니다. 게다가 적대자들은 피해자의 최종 호스트가 아닌 목표를 제안한 문헌에서 Kang [3]과 Studer [4]에 의해 공유 전송 링크를 공격하는 공격 방법론을, 우리가 전송 링크 DDoS라고 부르는 공격 방법론으로 전환했습니다. 더 나쁜 것은 실제로 전송 링크 공격이 훨씬 더 자주 발생하고 있으며, Akamai [5]에 따르면 2017년 3분기에 관찰된 공격의 99% 이상이 핵심 인터넷 인프라를 대상으로 하였으며, 응용 프로그램 계층은 1% 미만이었습니다.

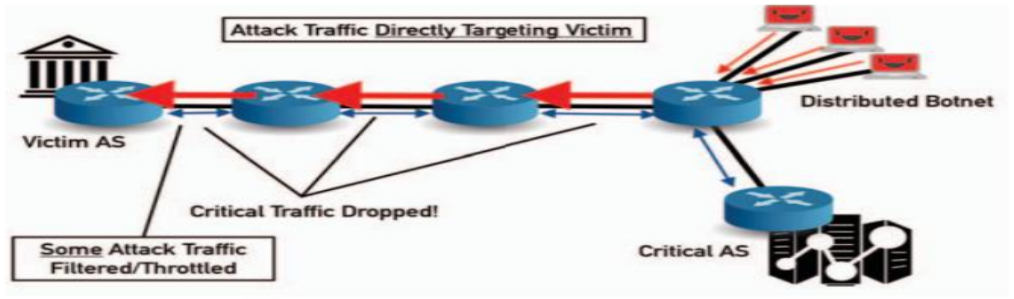
우리의 시스템인 Nyx는 현대적인 DDoS와 불리한 네트워크 상황을 해결하기 위해, 특히 다중 홈드 자치 시스템(AS)으로 분류되는 방어 또는 배포 네트워크가, 중요한 트래픽을 공격 트래픽과 경로 수준에서 격리시켜서 중요한 트래픽이 제한된 자원에 대해 악의적인 트래픽과 경쟁하지 않도록 합니다. 우리는 이를 위해 DDoS 완화를 필터링 문제가 아닌 라우팅 문제로 고려함으로써, 공격적인 트래픽의 양에 의존하지 않고도 DDoS 공격을 효과적으로 완화할 수 있는 Deployer AS라는 우리 시스템을 배치하는 자치 시스템의 능력을 향상시킵니다. 우리가 접근 방식을 전환한 동기는 현대적인 DDoS 공격이 종종 1 Tbps 이상의 지속적인 트래픽 수준에 도달하며, CDN 및 필터링 메커니즘이 효과적인 방어를 제공하지 못한다는 점입니다. 하지만 Nyx는 이러한 비용이 많이 드는 스트림별 필터링 결정 및 대역폭 경쟁을 피하고 더 확장 가능한 방어를 제공합니다. Nyx를 사용하는 배포자는 대규모 공격 흐름의 비용이 많이 드는 처리를 수행할 필요가 없으며, 우리 시스템은 알려진 중요한 네트워크에서의 양성 트래픽만을 관리하도록 초점을 맞추기 때문에 트래픽을 양성 또는 악성으로 분류할 필요가 없습니다. Nyx의 예제 배포 사례에는 국립 연구소의 슈퍼 컴퓨터와 같은 원격 컴퓨팅 리소스로부터의 트래픽 또는 스마트 그리드와 같은 중요한 사이버 물리 인프라에서의 트래픽을 보호하는 것이 포함됩니다. 우리의 목표를 달성하기 위해, Nyx는 외부 협조 없이도 라우팅 AS에서 Border Gateway Protocol (BGP)의 기존 기능을 활용하여 들어오는 중요한 트래픽의 경로 격리를 달성하므로 기존의 인터넷 라우팅 인프라에 배치할 수 있습니다.

먼저, 우리는 배포자 AS가 공격받는 링크에서 나가는 트래픽과 들어오는 트래픽을 성공적으로 조정하는 방법에 대해 다룹니다. 나가는 경로를 변경하는 것은 간단하지만, BGP는 목적지 네트워크가 들어오는 경로를 직접 제어할 수 있는 방법을 제공하지 않습니다. 우리는 이 제한을 극복하기 위해 대체 경로를 배포자 네트워크로 전파하고, 어떤 AS가 그러한 경로를 전파하는지를 전략적으로 유도된 BGP 루프 감지를 통해 제어합니다. 우리는 배포자가 제어할 수 없는 라우터에서 루프 감지를 달성하기 위해 광고된 경로에 나타나는 네트워크에 대해 선택적으로 거짓 정보를 제공함으로써 이 제한을 극복합니다. 저희가 Fraudulent Route Reverse Poisoning 또는 FRRP라고 부르는 우리의 트래픽 엔지니어링 기술은 RPKI와 같은 원산지 무결성 메커니즘을 도입한 라우터라도 작동합니다. Nyx는 대체 경로를 패킷 전달 측면에서 더 선호되도록 하기 위해 기존의 트래픽 엔지니어링 기술을 사용하며, FRRP를 활용하여 대체 경로가 DDoS 공격을 받는 링크 주변을 퍼지게 하지만 실제로 그 링크에 도달하지 않도록 합니다.

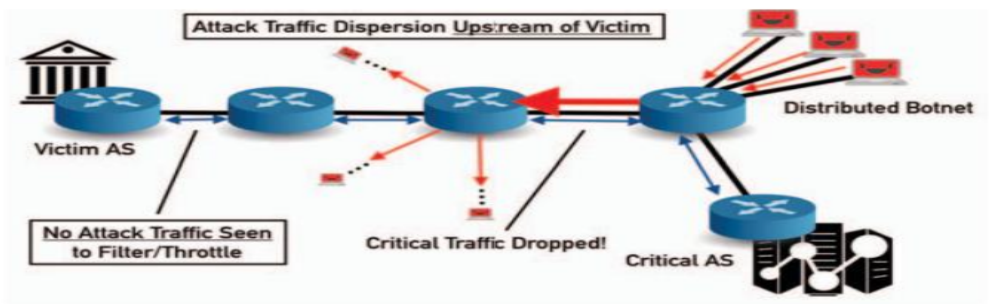
두 번째로, 우리의 배포자는 중요하지 않은 네트워크의 수를 제한해야 합니다. 이러한 중요하지 않은 네트워크들은 비판적인 네트워크가 사용하는 경로를 조정함으로써 최상의 경로를 변경할 수 있습니다. 이를 "방해"라고 정의하며, 방해는 두 가지 원하지 않는 시나리오를 초래할 수 있습니다. 주로, 방해는 악의적인 트래픽이 대체 경로를 통해 흐르게 하여 대체 경로 자체가 DDoS 공격을 받을 수 있습니다. 또한, 방해를 받은 네트워크가 공격 트래픽의 원천이 아니더라도, 선택된 중요 AS 이외의 AS로부터의 관련 없는 트래픽은 대체 경로를 혼잡시킬 수 있습니다. 이러한 방해를 완화하기 위해, 우리는 경로 전파 제어 기술을 확장하여 대체 경로를 비판적인 네트워크 및 대체 경로에 나타나는 네트워크 이외의 모든 네트워크로 전파하지 않도록 합니다.

마지막으로, 우리 시스템은 대체 경로가 비판적인 네트워크로부터의 트래픽과 방해를 받는 네트워크로부터의 트래픽을 처리할 충분한 여유 용량을 보유하고 있는지 보장해야 합니다. 우리 시스템은 대체 경로가 추가된 부하를 처리하는 데 어려움을 겪고 있는지를 감지하기 위해 TCP 흐름에서의 패킷 손실을 샘플링함으로써 이를 감지합니다. 그러면 시스템은 다른 대체 경로를 탐색하려고 시도할 것입니다. Nyx는 진화 알고리즘을 활용하여, 비판적 네트워크와의 TCP 세션에서 패킷 손실을 최소화하려는 적합성 함수를 사용합니다. Nyx는 대체 경로를 새로운 잠재적인 경로로 샘플링하기 위해 대체 경로를 철회하고 다시 전파하는 방식을 사용하여, 공격을 받는 링크와 이전 대체 경로의 혼잡한 링크에 경로를 전파하지 않고서만 가능한 대체 경로를 탐색합니다. 또한 Nyx는 악의적인 트래픽 소스(악의적인 봇이 포함된 AS)나 상위 링크의 실제 용량에 대한 지식이 필요하지 않습니다. 섹션 III에서 설명된 테이블 I과 II는 Nyx가 작동하기 위해 필요하거나 필요하지 않은 모든 정보를 요약합니다.

Nyx의 능력을 시뮬레이션을 통해 증명하며, 우리 시스템이 다양한 DDoS 공격 시나리오를 완화하려고 시도하는 현실적인 인터넷 규모의 시뮬레이션을 사용하여 이 세 가지 도전을 해결할 수 있는 능력을 보여줍니다. 우리는 배포 AS를 인터넷에 연결하는 주요 링크가 공격을 받는 경우(전통적인 DDoS라고 함)와 공격받은 링크가 배포자의 상위 레벨에 위치한 경우(강 및 스터더에 의해 Crossfire 및 Coremelt로 설명되는 트랜짓 링크 DDoS)를 포함한 경우에 대부분의 경우(98%)에서 비판적인 트래픽을 공격받는 링크를 피하고 대안 경로로 안전하게 라우팅할 수 있다는 것을 발견했습니다. 비판적이지 않은 네트워크의 최적 경로 변경을 제한하는 기술을 구현하면, 이전에 경로 축소 전략을 사용하기 전에 평균적으로 1000에서 5000개의 네트워크에 대한 무작위 경로 변경을 10개로 줄일 수 있습니다. 또한, 경로 길이에 추가 비용이 거의 발생하지 않고, 최적 경로가 경제적으로 불리한 경로로 전환되지 않는 것으로 나타났습니다. 마지막으로, 우리는 DDoS 공격 시나리오에 관계없이 98%의 경우에 들어오는 비판적인 트래픽을 대체 경로로 조정하여 혼잡이 크게 줄어든다는 것을 입증했으며, 트랜짓 링크 DDoS의 경우 98% 이상의 경우에 비판적인 트래픽을 완전히 혼잡하지 않은 경로로 이동할 수 있으며, 전통적인 DDoS의 경우 평균적으로 70% 이상의 시간에 비판적인 트래픽을 완전히 혼잡하지 않은 경로로 이동할 수 있다는 것을 발견했습니다.



[그림 1] 전통적인 DDoS: 피해 AS가 직접 공격 대상이 되는 경우



[그림 2] 트랜짓 링크 DDoS: 피해 AS의 상위에 있는 트랜짓 AS들이 공격 대상이 되지만 트래픽이 피해 AS로 전달되지 않는 경우

그림 1: 전통적인 DDoS와 트랜짓 링크 DDoS. 트랜짓 링크 DDoS의 경우, 2009년의 Coremelt [4] 공격과 CrossFire [3]에서 보여진 것처럼, 필터링과 throttling은 공격 트래픽이 피해자에 의해 전혀 볼 수 없기 때문에 수행할 수 없습니다.

이 논문의 나머지 부분은 다음과 같이 구성됩니다.

- 섹션 II: DDoS와 BGP에 대한 관련 배경을 제공합니다.
- 섹션 III: 우리 시스템 설계의 세부 사항을 제시합니다. 공격적인 모델, 설계 제약 조건, DDoS 완화 방법, 다루는 연구 도전 과제 및 완화 전략을 실현하는 메커니즘에 대해 다룹니다.
- 섹션 IV: 시뮬레이션 방법론의 세부 사항과 주장을 뒷받침하는 평가 결과를 다룹니다.
- 마지막으로, 섹션 V: 다른 DDoS 완화 시스템과 우리 시스템을 비교하고, 섹션 VI에서는 진행 중인 미래 연구에 대해 결론을 내립니다.

II. 배경A. DDoS와 봇넷부피 기반 분산 서비스 거부(DDoS) 공격: DDoS 공격은 기술적 복잡성이 낮은 대신 영향력이 높아서 최근 몇 년간 빈도가 증가하고 있습니다. 일반적으로 DDoS 공격은 인터넷의 감염된 호스트에서 시작되며, Conficker 봇넷 [17]과 같은 경우가 그렇습니다. 그러나 새로운 봇넷은 주로 IoT 기반 장치에서 시작되며, Mirai [1]와 같은 것이 있습니다. 출처가 변화함에 따라 감시 조직들은 2015년부터 2016년까지 전체 DDoS 사건이 83% 증가했다고 보고했습니다. 더욱 문제인 것은 적대자가 DDoS 공격을 수행하기 위해 이용할 수 있는 대역폭이 연간 꾸준히 증가하고 있다는 것입니다. 연구자들은 2015년부터 2016년까지 100Gbps 이상의 공격이 140% 이상 증가했다고 관찰했으며, Mirai는 여러 차례에 걸쳐 1 Tbps 이상의 악의적인 트래픽을 생성했습니다. 역사적으로, 호스트에서 주로 시작된 전통적인 DDoS 공격은 적대자가 봇 트래픽을 피해자 네트워크로 직접 보내어 피해자 네트워크의 가장자리에서 트래픽을 삭제하도록 하여 서비스 품질을 심각하게 저하시킵니다. 이 논문 전반에 걸쳐서 우리는 Nyx가 그림 1a에 설명된 전통적인 DDoS에 대응하는 방법에 대해 논의할 것입니다.

트랜짓 링크 DDoS: 최근에 새로운 DDoS 공격 전략이 등장하여, 피해 호스트의 전체 네트워크를 제공하는 핵심 트랜짓 링크를 공격하는 것을 보여주는 전략이 나타났습니다. 이를 "트랜짓 링크 DDoS"라고 하며, 그림 1b에서 자세히 설명되어 있습니다. 실제로 트랜짓 링크 DDoS는 최근에 주요 DNS 제공업체인 Dyn [19], 유명한 보안 저널리스트인 Bryan Krebs의 KrebsOnSecurity [20], 그리고 리베리아 국가 [2]를 공격한 사례에서 관찰되었습니다. 트랜짓 링크 DDoS에서 적대자는 피해자의 실제 네트워크의 상위로 봇 트래픽을 유도하여 목표로 하는 트래픽이 최종 목적지에 도달하기 훨씬 앞서서 삭제되도록 합니다. 이 경우 봇들은 피해자가 아닌 다른 네트워크로 트래픽을 보내기 때문에 피해자는 트래픽을 필터링하거나 블랙홀로 처리할 수 없습니다. 이러한 공격의 예는 Coremelt 공격 [4] 및 Crossfire 공격 [3]이 있습니다. Coremelt 공격은 트랜짓 링크 DDoS 공격으로, 공격에 참여하는 N개의 봇들 간에 N^2개의 연결을 설정하여 인터넷의 트랜짓 코어에 심각한 피해를 입힙니다. Coremelt가 처음 소개된 당시에는 다른 트랜짓 링크 DDoS 공격이 존재하지 않았지만, 그 이후에 Crossfire 공격과 같은 다른 공격이 나타났습니다. Crossfire는 Coremelt와 유사한 방식으로 공격 트래픽이 예상되는 "원하는" 위치로 트래픽을 유도하여 선택된 공격 경로를 통해 공격 트래픽이 타겟 AS에 의해 절대 삭제되거나 필터링되지 않도록 합니다. 이렇게 함으로써 Crossfire는 단순히 사용 가능한 용량을 과부하시켜 트랜짓 코어의 중요한 서버 연결을 끊을 수 있습니다. Nyx는 전통적인 DDoS로 인한 혼잡을 우회하는 것 외에도 트랜짓 링크 DDoS에도 대응하여, 거의 모든 경우에 단일 중요 AS의 공격으로 인한 혼잡을 완화합니다. 이에 대해 더 자세히는 다음 섹션인 섹션 III에서 논의할 것입니다.

B. 경계 게이트웨이 프로토콜과 AS 간 라우팅
Nyx의 작동 방식을 논의하기 전에, 여러 십년 동안 최고의 기대를 뛰어넘는 성능을 발휘해 온 인터넷 라우팅 인프라를 검토합니다. 오늘날 현대 인터넷은 여러 개의 자율 시스템(AS)으로 구성되어 있으며, 각 AS는 특정 관리적 통제 아래의 라우터와 IP 주소 집합입니다 [21]. 인터넷 상의 AS 간에는 경계 게이트웨이 프로토콜(BGP) [22]이 사실상의 라우팅 프로토콜로 사용됩니다. BGP는 IP 주소 블록에 대한 경로 정보를 AS 간에 교환하여 각 AS가 목적지로 패킷을 전달하는 방법에 대해 알 수 있도록 합니다. BGP는 경로-벡터 라우팅 프로토콜이며 정책을 갖추고 있습니다. 이는 경로가 이동하는 경로와 다른 품질을 포함하고, 개별 라우터는 가장 좋은 경로를 정의하고 선호하는 경로를 사용하여 패킷을 전달할 수 있습니다. BGP 정책은 종종 단순히 가장 빠르거나 가장 짧은 경로를 선택하는 것을 넘어서 복잡하고 유연한 AS 간 관계에 기반한 결정을 가능하게 합니다. 이 결정 프로세스는 라우터에게 AS별로 트래픽을 어디로 보낼지 알려주며, 각 차례의 점프에서 BGP 라우터들은 자체 정책에 따라 선택된 다른 AS를 통해 목적지로 향하는 트래픽을 수신하고 전달합니다.
이 작업에서 매우 중요한 BGP 트래픽 엔지니어링 기술 중 하나는 홀-펀칭(hole-punching) [22], [23]입니다. 홀-펀칭에서는 라우터가 IP 주소 블록과 해당 블록의 해체를 모두 광고하는데, 각각은 다른 경로 특성을 가집니다. 이 IP 블록들은 기술적으로 다르기 때문에 BGP는 이들을 서로 다른 목적지 경로로 취급하여 특정 IP 주소 블록에 대해 보다 구체적인 정책을 사용할 수 있습니다. 이러한 보다 구체적인 경로는 항상 가장 구체적으로 일치하는 IP 블록을 기반으로 라우터가 사용하게 됩니다. 우리는 섹션 III-B에서 홀-펀칭에 대해 더 자세히 논의할 것입니다.

III. 시스템 설계A. 혼잡 회피 라우팅트랜짓 링크 DDoS로 인한 해결되지 않은 위협과 전통적인 DDoS를 완화하기 위해 Nyx를 설계했습니다. Nyx는 DDoS 공격으로 인해 손상된 링크를 우회하거나 다른 악화된 네트워크 상황에서 Nyx 배포자와 사전에 알려진 중요 AS 간의 트래픽을 라우팅함으로써 DDoS 공격을 완화합니다. 높은 수준에서 Nyx는 중요 네트워크와의 네트워크 성능에 관련된 공격 트래픽을 무시하여 필터링이 필요 없게 만듭니다. Nyx는 경로 단위로 작동하여 비용이 많이 들고 어려운 각 스트림 결정을 내리지 않아도 됩니다. Nyx는 배포자의 BGP 라우터와만 직접 상호 작용하며, DDoS 우회 라우팅 시 중요 AS를 포함하여 외부 협력을 받지 않습니다. Nyx는 배포자가 소유한 IP 주소에 대한 라우팅 광고만을 생성하므로 다른 AS의 라우팅 정보에 악영향을 미치지 않습니다. Nyx의 혼잡을 우회하고 공격 트래픽을 무시할 수 있는 능력은 전통적인 DDoS의 경우 그림 2에서, 트랜짓 링크 DDoS의 경우 그림 3에서 설명되어 있습니다. 하지만 이 섹션의 나머지 부분에서 Nyx가 어떻게 작동하는지에 대해 자세히 설명하겠습니다.Nyx가 배포되는 방법에 대해 논의하기 전에 이전 솔루션이 충분하지 않은 이유를 고려해 보겠습니다. 트래픽 필터링 및 우선 순위 지정은 다중 Tbps 트래픽 흐름을 가진 현대 DDoS에 대해 효과가 없습니다. 또한 문헌에서 제안된 트랜짓 링크 DDoS 공격(예: Crossfire 및 Coremelt [3], [4])과 리베리아 [2] 등에서 관찰된 현실 세계 공격은 공격 트래픽을 직접 대상 AS로 보내지 않습니다. 이 트랜짓 링크 DDoS의 특성으로 인해 피해자는 수신 트래픽에 어떠한 필터링도 적용할 수 없습니다. 왜냐하면 중요 트래픽이 상위 계층에서 삭제되며 일반적으로 피해자 AS의 제어 범위를 벗어나기 때문입니다. Nyx는 필터링이나 우선 순위 지정 기술에 의존하지 않고 오직 양호한 트래픽에 대한 제어를 통해 이 문제를 다르게 접근합니다. 우리

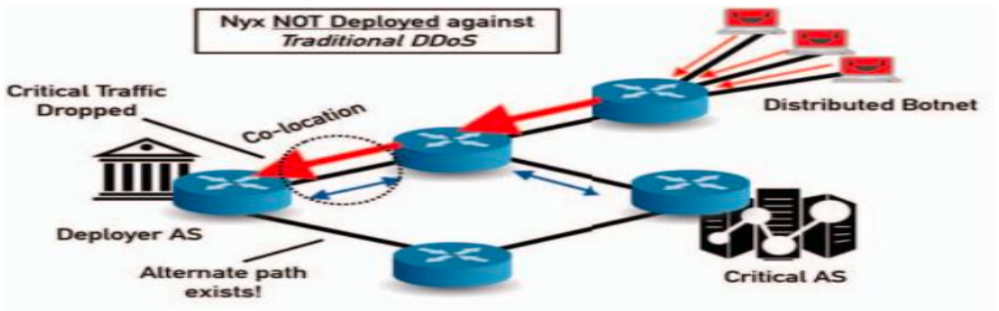
시스템은 경로 선택 문제에 초점을 맞추므로 Nyx는 혼잡과 DDoS 공격을 우회하기 위해 일반 BGP 및 트래픽 엔지니어링 기술을 활용할 수 있습니다. 이렇게 함으로써 배포자가 다중 Tbps 공격을 받을 때도 수신 품질을 유지하면서 상위 AS와 통신할 수 있게 됩니다.

1. 현실적인 배포: 트랜짓 링크 DDoS를 대역폭 계약을 통해 완화하는 이전 시스템과는 달리, Nyx는 중요 AS를 포함한 다른 AS로부터 외부 협력을 요구하지 않습니다. 또한 Nyx는 공격자가 어디에서 시작되었는지에 대한 정보를 알 필요가 없습니다. Nyx는 오직 CAIDA [24]의 오픈 소스 데이터를 통해 AS 간의 관계를 알고 있다고 가정합니다. 더 자세한 내용은 부록의 표 I 및 표 II에 Nyx가 필요로 하는 정보 및 필요하지 않은 정보를 요약해 두었습니다.

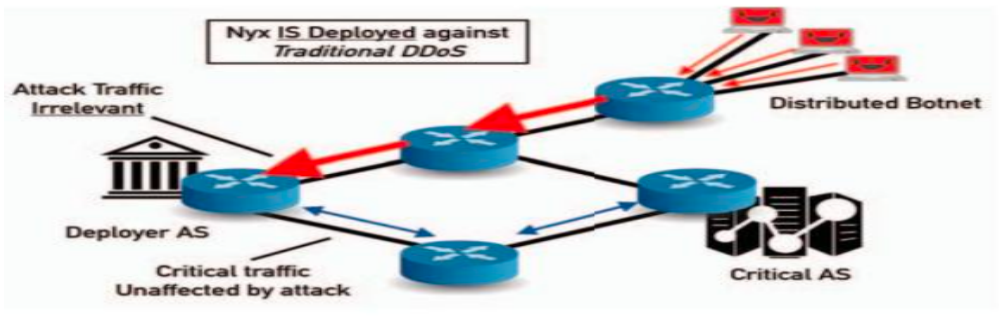
우리 시스템은 또한 네트워크 토폴로지에서 봇의 위치나 DDoS 공격 흐름의 형태에 대한 지식이 없습니다. 대신, Nyx는 지속적으로 패킷 흐름 성능을 사용하여 중요 AS와 배포자 AS 사이의 현재 경로가 혼잡한지를 나타냅니다. 또한, Nyx는 인터넷 링크의 대역폭이나 용량에 대한 정보를 필요로하지 않습니다. 이 작업에서 Nyx를 검증하기 위해 사용되는 시뮬레이터는 토폴로지 내 링크 용량에 대한 대역폭 모델을 사용하지만 이 정보는 배포자 AS나 Nyx에게 알려져 있지 않습니다. Nyx는 패킷 흐름 성능을 사용하여 현재 경로가 혼잡함을 감지하면 혼잡을 우회하고 충분한 용량을 갖춘 대체 경로를 발견하기 위해 진화 알고리즘을 사용합니다. 마지막으로 Nyx는 개별 트래픽 흐름이 악의적인지 또는 양호한지 여부를 알 필요가 없습니다. Nyx 배포자는 중요 AS를 미리 알고 있으며 해당 AS에서 수신되는 모든 트래픽을 "양호"로 처리합니다. 배포자 AS가 다중 연결되어 있는 경우(Nyx에게 특성을 제공하는), 실제 DDoS 이벤트나 다른 악화된 네트워크 조건의 영향에서 벗어난 경로로 중요 AS에서의 트래픽을 강제로 전환함으로써 악의적인 트래픽은 배포자에게 완전히 관계없게 됩니다. 이것이 Nyx가 트랜짓 링크 및 전통적인 DDoS를 완화할 때 봇넷 규모 독립성 특성을 제공하는 요인입니다.
Nyx가 알고 있는 정보와 모르는 정보를 넘어서, 우리는 Nyx 배포의 다음과 같은 가정을 실제 실제 배포에 대해 검증하고 이러한 가정을 나중에 섹션 IV에서 확인합니다:

Nyx가 필요한 것은 방어하는 AS가 Nyx를 배포하는 것뿐이어야 합니다. 이는 우리의 시스템이 인터넷 전체에 걸쳐 완전히 배포되어야만 작동한다는 의존을 의미하지 않습니다. 따라서 우리의 중요 AS는 수비자에게 어떤 지원도 제공하지 않습니다.
• Nyx는 다른 AS에 부정적인 영향을 미치지 않아야 합니다. Nyx는 수비자와 왕래하는 경로 이외의 경로를 변경해서는 안 됩니다.• Nyx는 다른 AS의 일반적인 활동에 심각한 영향을 주지 않아야 합니다. 우리의 기술을 활용하기 위해 AS 운영자는 배포 AS의 BGP 스피커를 제어할 수 있어야 합니다.• Nyx는 BGP에 어떠한 변경도 필요로 하지 않아야 합니다. 왜냐하면 우리가 개발한 기술을 통해 알려진 중요 AS에서의 들어오는 트래픽을 조정할 수 있기 때문에 이 작업은 배포 AS의 라우팅 정책 조정만으로 수행될 수 있습니다.

2. 적대적 모델: 전통적인 DDoS 및 트랜짓 링크 DDoS가 일반적으로 제어되는 방식에 따라, 우리의 적대자는 기본 네트워크 구조를 제어하지 않으며 라우팅에 대한 인식이 없으므로 라우팅 결정을 내릴 수 없습니다. 대신, 우리의 위협 모델은 분산된 대규모 봇넷이나 멀티-Tbps 공격 흐름을 생성할 수 있는 호스트 하위 집합을 제어하는 지능적인 적대자를 고려합니다. 이 제한을 통해 적대자는 특정 공격을 위해 봇을 선택하고, 인터넷 전체에 분산된 봇들이 얼마나 많은 트래픽을 보낼 것인지, 그리고 각 봇이 그 트래픽을 전송해야 하는 인터넷 전체 토폴로지의 어디로 보내야 하는지를 제어할 수 있습니다. 현재의 적대적 모델에서 우리는 Nyx 설계에서 전역 적대자를 고려하지 않았습니다. 그러나 우리는 섹션 VI에서 이 문제를 해결하기 위한 진행 중인 작업에 대해 논의할 것입니다. 부록의 표 I 및 표 II에서 보았듯이 Nyx는 봇 AS가 어디에 위치하는지, 특정 공격에 대해 얼마나 많은 트래픽을 보내고 있는지, 또는 특정 공격에 악의적인 봇의 수를 알지 못합니다.



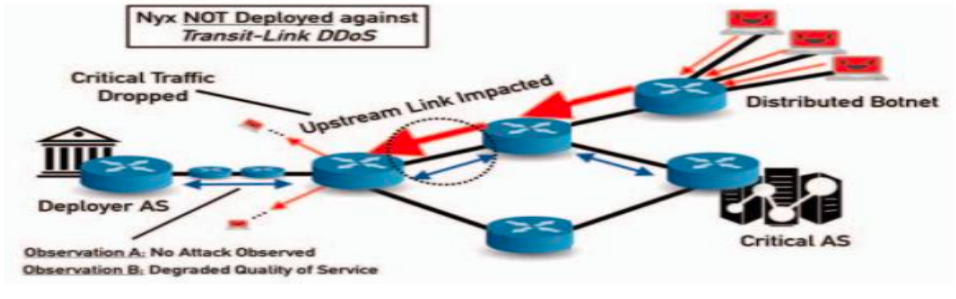
[그림 3] (a) Nyx를 배포하지 않음



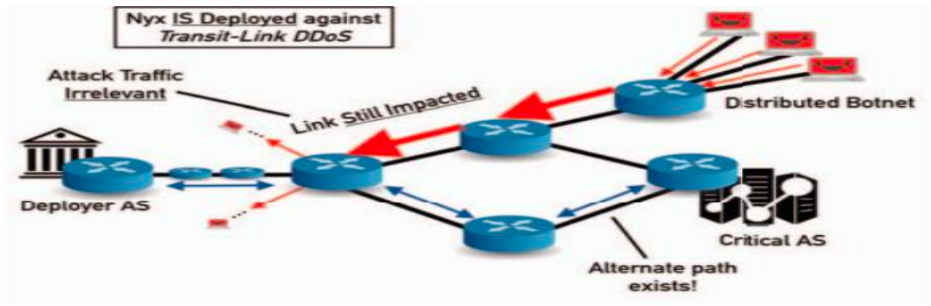
[그림 4] (b) Nyx를 배포함

Fig. 2: 전통적인 DDoS에 대한 Nyx 배포

==========



[그림 5] (a) Nyx를 배포하지 않음



[그림 6] (b) Nyx를 배포함

Fig. 3: 트랜짓 링크 DDoS에 대한 Nyx 배포

==========

이 섹션의 나머지 부분에서는 Nyx가 배포 가능성과 내구성을 보장하기 위해 설정한 디자인 제한 내에서 세 가지 핵심 목표를 달성하는 방법을 탐구할 것입니다. Nyx가 다루는 첫 번째 문제는 상류의 중요 AS에서 들어오는 트래픽을 대체 경로로 조정하는 방법이며, 이에 대해 다음 섹션인 III-B에서 논의됩니다. Nyx가 해결하는 두 번째 도전은 III-C에서 다루는데, 여기서 disturbance는 주요 AS 외부의 AS 및 대안 경로 상의 AS가 새로운 경로로 전환되는 경우를 의미합니다. Nyx가 다루는 세 번째 도전은 III-D에서 논의되는데, 여기서 Nyx가 새로운 대체 경로가 중요 트래픽을 처리할 충분한 용량을 가진 경우의 수를 최대화하려고 시도하는 방법을 설명합니다.

B. 중요 트래픽 이전

Section II-B에서 언급한 것처럼 AS에서 나가는 트래픽은 BGP 로컬 우선 순위를 통해 조정하기가 간단하지만, AS로 들어오는 트래픽이 특정 AS 간의 조정을 통해서만 가능할 수 있습니다. SCION 및 SIBRA와 같은 제안된 시스템은 DDoS에 효과적으로 대응하기 위해 이러한 조정이 필요합니다 [15], [16]. 그러나 Nyx는 배포 AS와 다른 AS, 특히 중요 AS 간의 조정이 없다고 가정합니다. 배포 AS는 DDoS 공격 및 기타 악화된 네트워크 상태를 피할 수 있는 링크를 거쳐서만 중요 AS가 이동할 수 있는 AS 수준의 경로를 제한할 수 있습니다. 이것은 우리가 해결해야 할 첫 번째 중요한 도전 과제를 제시합니다: Nyx는 협력 없이도 어떻게 DDoS 트래픽을 피해서 AS로 들어오는 트래픽을 경로 설정할까요?

배포 AS에게 중요 AS가 따를 수 있는 AS 수준의 경로를 특정 경로로 제한함으로써, Nyx는 인터넷 라우팅 인프라를 재설계하지 않고도 Scion 및 SIBRA와 동일한 이점을 얻을 수 있습니다. 혼잡을 피하기 위해 이러한 경로는 전통적 또는 트랜짓 링크 DDoS 공격에 영향을 받은 혼잡하거나 공격받은 링크를 통과해서는 안 됩니다. Nyx는 이를 통해 중요 AS의 다른 AS들과의 연결성을 제한하지 않고, 중요 AS가 배포 AS 이외의 AS들로부터 받는 BGP 광고를 감소시키지 않습니다. 고수준에서 Nyx는 공격 트래픽을 무시할 수 있게 만드는 기존 라우팅 기능을 사용합니다. Figures 2와 3에서 설명된 것처럼, 배포 AS로 향하는 중요 트래픽이 혼잡하지 않은 대체 경로로 강제되므로, DDoS 또는 링크 장애와 같은 모든 악화된 조건으로 인한 혼잡은 더 이상 문제가 되지 않습니다.

배포 AS에게 이러한 능력을 부여하기 위해 우리는 Fraudulent Route Reverse Poisoning(FRRP)이라는 전략을 개발했습니다. Nyx는 FRRP를 사용하여 배포 AS에서 시작된 경로 광고가 중요 AS에 전파될 때 혼잡하거나 DDoS 또는 링크 장애 또는 대역폭 사용 증가로 인한 혼잡과 같은 악화된 조건을 통과하지 않도록 보장합니다. FRRP는 중요 AS의 로컬 우선 순위를 변경하지 않고, 대신 배포 AS에서 시작된 광고에 공격당한 링크가 포함되지 않도록 하여 배포 AS로 향하는 아웃바운드 트래픽을 중요 AS가 공격당한 링크를 통해 경유하도록 하는 선택권을 박탈합니다. 이러한 혼잡한 링크를 배포 AS에 대한 연결로 사용할 수 없도록 함으로써 중요 AS는 배포 AS로 트래픽을 보내는 대체 경로를 선택합니다. 이렇게 하면 배포 AS는 중요 AS에서 생성된 경로 광고를 조작함으로써 중요 AS로부터 들어오는 트래픽을 제어할 수 있습니다.

자세히 설명하면, FRRP는 Figure 4에 나와 있는 것처럼 작동합니다. 중요 AS 3에서 배포 AS 1로의 일반 트래픽은 일반적으로 중요 AS가 AS 2를 통해 AS 3에서 배포 AS로 흐르게 됩니다. 그러나 공격 트래픽으로 인해 3에서 2로 향하는 링크가 혼잡해졌습니다. 이 링크를 피하고 AS 4를 통해 중요 트래픽을 라우팅하기 위해 배포 AS는 경로에 AS 2를 추가하여 BGP 광고를 속입니다. 또한 배포 AS는 경로 끝에 자신의 AS 번호를 추가하여, 나중에 배포된 RPKI에서 FRRP가 작동할 수 있도록 합니다. AS 4가 이 경로를 받으면 중요 AS 3에게 경로를 광고합니다. AS 2가 배포 AS에서 광고된 경로를 볼 때 BGP의 내장 루프 감지로 인해 AS 2는 AS 1에 의해 광고된 경로를 AS 3에 전달하지 않게 됩니다. 따라서 중요 AS 3은 더 이상 2를 통해 1로의 경로를 보지 않게 되고, AS 4를 통해 유일하게 사용 가능한 다른 경로를 사용하게 됩니다. Nyx는 적어도 하나 이상의 대체 경로가 존재하는 경우, 선택된 중요 AS로부터 들어오는 트래픽을 대체 경로로 라우팅하기 위해 FRRP를 활용합니다.

RPKI에서 FRRP 사용: FRRP를 사용할 때 적절하게 배치된 자원 공개 키 인프라(RPKI) 또는 자원 인증으로 알려진 것은 일반적으로 잘못된 경로 광고를 방지합니다. 그러나 Nyx는 Nyx에서 사용하는 전략적인 거짓말이 경로 원본 프로세스에 간섭하지 않도록 RPKI의 영향을 해결합니다. 구체적으로, 원천 자율 시스템 AS_{orig}와 루프 감지를 통해 피해야 할 AS 집합 $AV_{AS} = \{ AS_{AV1}, AS_{AV2}, ..., AS_{AVN} \}$ 이 주어진 경우, 배포자(이 경우 발신자)는 FRRP를 사용할 때 다음 경로를 광고합니다:

$$\{\, AS_{orig},\ AS_{AV_1},\ AS_{AV_2}, \ldots,\ AS_{AV_N}, \underbrace{AV_{orig}}_{\text{For RPKI}} \} \qquad (1)$$

이 새로운 경로는 목적지인 AS_{orig}에서 시작하여 피해야 할 AS들이 끝에 추가되고, 그 다음에는 다시 원천 또는 배포자 AS인 AS1을 거쳐 네트워크를 통해 전파됩니다.

$$\{ \underbrace{AS_3,\ AS_2,\ AS_1}_{\text{Actual Path}},\ \overbrace{AS_{orig}}^{\text{Packet at Dest}}\ , \underbrace{AS_{AV_1}, \ldots,\ AS_{AV_N}, AS_{orig}}_{\text{Irrelevant for Forwarding}} \} \qquad (2)$$

이러한 경우, 경로가 방출자에 의해 방출되는 동안 RPKI는 경로를 유효하게 취급할 것입니다. 왜냐하면 RPKI는 경로를 발생시킨 AS가 경로의 마지막 AS인지를 확인하기 때문입니다. 방정식 2에서 경로가 네트워크를 통해 확장됨에 따라 경로를 따라 이동하는 동안, 경로에 포함된 AS들은 발생자가 계속해서 경로에 포함되어 있기만 하면 계속해서 경로를 전달할 것입니다. 발생자 이후에 나오는 피해야 할 AS들은 전달과는 무관하며, 이 추가적인 AS들은 새로운 경로를 수신할 때 BGP 루프 감지의 메커니즘으로 인해 해당 경로를 사용하지 않을 것입니다. BGP 라우터는 자신의 AS 번호를 전체 경로에서 검사하고, 자신의 AS 번호를 발견하면 해당 경로를 삭제할 것입니다.

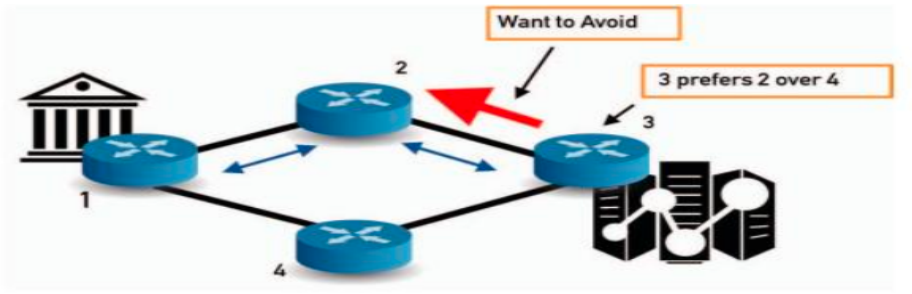
1. FRRP 및 네트워크 연결: 네트워크 연결을 유지하기 위해 배포자는 여전히 정상적인 경로를 광고하나, FRRP 경로는 앞서 섹션 II-B에서 설명한 홀 펀칭된 접두어들이 될 것입니다. 배포자는 임계 AS 이외의 AS와의 연결성을 유지하기 위해 정상적인 집합을 광고할 것이며, FRRP는 홀 펀칭을 통해 디-어그리게이트된 광고를 활용할 것입니다. FRRP는 더 많은 부하를 처리할 수 있는 대체 경로를 제공하여, Nyx를 실행하는 배포자가 임계 AS로부터 수신되는 트래픽을 성공적으로 조작할 수 있도록 합니다.

이 섹션에서 FRRP는 DDoS 공격 및 부적절한 네트워크 조건을 피할 수 있는 능력을 Nyx에 부여합니다. 대체 경로가 추가된 부하를 처리할 수 있는지 여부는 섹션 III-D에서 자세히 다룰 것입니다. 이 문제를 탐색하기 전에, 우리는 먼저 FRRP 사용의 부작용을 줄이는 Nyx의 능력을 살펴보겠습니다.

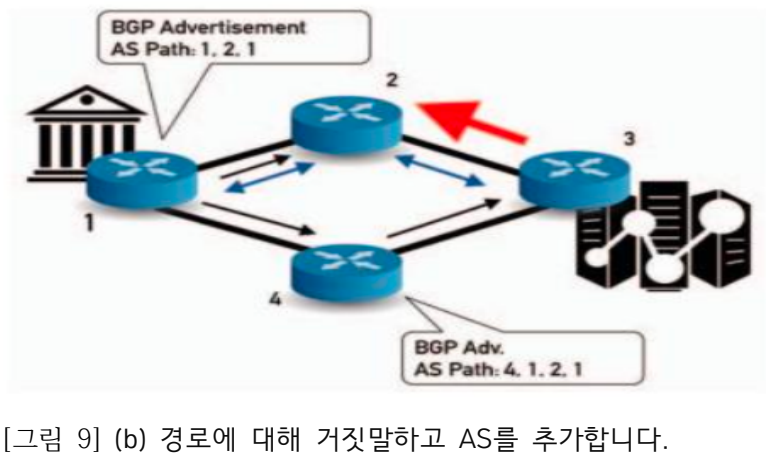
FRRP를 사용하면 임계 AS 이외의 AS의 배포자에 대한 우선 경로를 의도하지 않게 변경할 수 있습니다. 최악의 경우, 대량의 봇을 포함하는 AS의 경로가 변경되어 이제 DDoS 트래픽이 대체 경로를 통해 흐를 수 있습니다. 우리는 이러한 효과를 "disturbance"라고 합니다. disturbance를 해결하기 위해 FRRP 프로세스를 수정하는 두 가지 기술을 구현했습니다.

- 선택적 광고: 우리는 먼저 FRRP 경로를 광고하고, 임계 AS에서 배포자로의 가장 선호하는 대체 경로를 주의하고 기록합니다. 그런 다음 FRRP 경로를 철회하고, 이 경로를 임계 AS에서 배포자와 직접 연결된 첫 번째 AS에만 다시 광고합니다. 이상적으로 이렇게 함으로써 배포자의 라우팅 테이블에서 다른 관련 없는 경로로의 광고 전파를 방지할 수 있습니다.

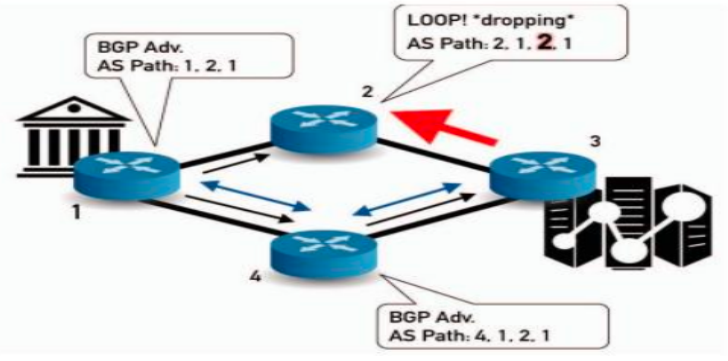
- Path Lining는 선호하는 대체 경로를 사용하여 FRRP를 활용하여 경로에 인접한 각 AS 및 그들의 고객 그룹에서 루프 감지를 트리거합니다. 그러나 경로에 있는 AS는 루프 감지를 하지 않습니다. 관련 없는 AS가 임계 AS를 위해 만든 경로를 삭제하도록 하는 것으로 대체 경로의 전파를 중지하여 disturbance를



[그림 8] (a) 핵심 링크가 혼잡 상태입니다.



[그림 9] (b) 경로에 대해 거짓말하고 AS를 추가합니다.



[그림 10] (c) 루프 감지가 트리거되었고 이제 피해야 할 핵심 AS가 대체 경로를 통해 통과합니다.

감소시킵니다. Path Lining은 배포자 외부의 AS들로부터 외부 협력이나 조정을 필요로 하지 않습니다. 배포자는 단순히 사기적인 광고에 루프 감지를 트리거하기를 원하는 AS들을 포함하여 이 경로를 수신하는 경우 이러한 AS들이 혼잡한 링크를 따라 있었던 것처럼 경로를 삭제하도록 요청합니다.

그림 4: Fraudulent Route Reverse Poisoning (FRRP)

==========

다수의 핵심 AS의 트래픽을 보호하려는 경우, deployer가 경로를 보호하는 방식은 직선적인 경로가 아닌 트리 구조를 형성할 수 있습니다. 다수의 핵심 AS를 보호하는 방법은 계속 진행 중인 연구로, 섹션 VI에서 논의합니다.

우리의 평가에서는 선택적 광고만 FRRP로 인한 장애를 실제로 증가시키는 경향이 있습니다. 이는 경로가 토폴로지를 통해 전파되는 방식의 부산물입니다. 그러나 경로 정렬은 FRRP에 의한 장애를 방지합니다. 왜냐하면 BGP 루프 감지로 인해 경로를 전파하지 않고자하는 AS를 목록에 추가할 수 있기 때문입니다. 경로 정렬을 사용하면 deployer의 조치로 인해 평균적으로 10개 미만의 AS에만 장애가 발생하며, 이에 대해 Section IV-B2에서 자세히 논의할 것입니다.

성능이 우수한 경로를 찾기 위한 방법으로, 우리 시스템은 원하는 AS들을 피하면서도 새로운 경로가 사용 가능한 대역폭과 관련하여 최적이 아닐 수 있습니다. 트래픽을 한 경로에서 다른 경로로 옮기면, 새로운 경로는 원래의 트래픽과 함께 핵심 AS 및 모든 영향을 받는 AS의 트래픽을 추가로 수용해야 합니다. 새로운 링크가 추가된 대역폭을 지원할 수 없는 경우, 여전히 혼잡이 발생할 수 있으며, Nyx를 사용하지 않은 것보다 더 나쁜 상황에 놓일 수도 있습니다.

트래픽을 충분한 대역폭 용량을 갖춘 새로운 링크로 옮기는 문제에 대응하기 위해, 우리는 대안 경로가 존재할 때 가장 성능이 우수한 경로를 찾기 위한 검색 알고리즘을 개발했습니다. 이 알고리즘은 FRRP와 경로 정렬을 반복적으로 사용하여 핵심 트래픽을 대체 경로로 이동시킵니다. 새로운 대안 경로가 사용될 때마다, 각 경로는 혼잡이 완화되었는지 여부를 평가하기 위해 사용됩니다.

Nyx에 의해 적용된 검색 알고리즘은 진화 알고리즘입니다. 여기서 적합성 함수는 각 대체 경로에서 핵심 AS의 트래픽에 따른 패킷 손실 성능입니다. 검색 중에 대체 경로가 혼잡 상태인 경우, Nyx는 대체 경로를 철회하고, 다시 FRRP와 경로 정렬 과정을 반복하면서 이전 대안 경로의 링크를 또한 DDoS 상태로 취급합니다. 이렇게 하면 핵심 AS가 부적합한 대체 경로를 통해 deployer AS의 트래픽을 라우팅하지 않습니다. 결국 Nyx는 DDoS 상태인 링크를 우회하고 성능이 우수한 대체 경로를 제공하지 못한 링크를 제외하면서 대안 경로 생성 과정을 반복합니다.

IV. 평가

Nyx의 효과에 대해 알아야 할 많은 질문이 있습니다. Nyx가 수신 중인 중요한 트래픽을 혼잡 상태에서 다른 대안 경로로 이동할 수 있을까요? Nyx는 이를 수행하는 동안, deployer 및 critical AS와 관련이 없는 AS의 BGP 결정 및 상태에 영향을 주지 않고 작동할 수 있을까요? 대안 경로의 경로 길이는 증가할까요, 그리고 얼마나 될까요? Nyx는 단순히 트래픽 이동을 넘어서서 중요한 트래픽을 완전히 혼잡하지 않은 링크로 또는 적어도 덜 혼잡한 링크로 라우팅할 수 있을까요? Nyx의 혼잡 회피 능력은 공격자의 봇넷 선택, deployer 및 critical AS 간 링크 용량, 인터넷의 다양한 토폴로지에 무관할까요? 마지막으로, Nyx는 외부 협조 없이 단일 멀티 홈 AS에만 배치되어서 모든 것을 수행할 수 있을까요?

이러한 질문에 대답하기 위해 우리는 이벤트 기반의 이산 네트워크 시뮬레이터를 구축하여 인터넷에서 라우터 및 트래픽 흐름의 특성과 기능을 모델링했습니다. Nyx의 평가는 복잡성이 매우 높기 때문에 시뮬레이터의 설계가 어려웠습니다. Nyx의 주장된 속성들만 평가하는 것뿐만 아니라 AS, BGP 라우터 정책, BGP 라우터, 라우터 간의 실제 토폴로지 링크, 공격자가 사용하는 봇넷 및 대역폭 모델 등 많은 다양한 요소들을 모델링해야 했습니다.

A. 시뮬레이터 설계

이 섹션에서는 이전에 Schuchard 등이 수행한 작업에서 사용된 시뮬레이터 설계 선택 사항을 탐색합니다 [26], [27]. 완전히 정확한 시뮬레이션을 위해 필요한 인터넷의 많은 속성들은 실제 트래픽 흐름, AS 간 링크의 대역폭 용량, 한 링크를 다른 링크보다 사용하는데 드는 비용 등과 같은 정보들은 엄격하게 보호되는 비밀입니다. 그러나 네트워크의 근사적이고 최신의 토폴로지와 봇넷 분포와 같은 다른 속성은 신뢰할 수 있는 공개 소스에서 얻을 수 있습니다. 시뮬레이터가 사용하는 정보에 대해 논의하고, 혼잡을 피하면서 경로를 찾을 때 Nyx가 알지 못하는 정보를 정리한 Table IV-A가 부록에 있습니다.

1. 네트워크 토폴로지: 인터넷의 토폴로지를 모델링하기 위해 CAIDA가 제공하는 방대한 양의 정보, 특히 그들의 AS 추론 관계 데이터셋 [24]을 활용합니다. CAIDA의 추정된 토폴로지를 사용하여 2016년 말부터 2017년 중반까지의 각 AS를 소프트웨어 라우터로 모델링하고, 각 AS는 실제에서 사용되는 라우팅 정책에서 가져온 현실적인 설정으로 BGP를 사용합니다. 시뮬레이션된 라우터가 사용하는 BGP 정책은 운영자들이 사용하는 최상의 실천 방법에 맞추어져 있으며, 표준화된 BGP 결정 프로세스에 의존합니다 [22]. 이전에 설명한 대로, 각 AS는 그 자체로 다양한 네트워크입니다. Nyx는 AS 수준의 혼잡 회피에 관심이 있으므로 AS 내부의 라우팅 역학을 크게 무시할 수 있습니다. AS 내부를 시뮬레이션하더라도, 최신 인터넷에서는 AS 내부의 엔드 호스트가 스스로를 방어해도 transit-link DDoS 공격이 효과적으로 작동합니다. 앞서 언급한 Scion과 SIBRA와 같은 기존 시스템은 엔드 호스트가 대역폭 예약을 제어할 수 있게 해주지만, 이러한 시스템은 핵심 인터넷 인프라를 재설계하고 다시 배포해야 모든 이점을 제공합니다. 이 섹션의 나머지 부분에서 Nyx가 핵심 인터넷 인프라의 변경이나 다른 AS의 참여 없이도 대역폭 예약 시스템인 SIBRA와 동일한 보장을 제공한다는 것을 증명할 것입니다.

2. 대역폭 모델: 현대 인터넷의 불변의 대역폭 모델을 수립하는 것은 여러 논문에 가치 있는 미해결된 문제임을 인식합니다. 따라서 우리는 효과적으로 대역폭 용량을 할당할 수 있는 정확하고 일반적인 모델을 개발하고 시험했습니다. 이 모델을 통해 이러한 링크에 대한 공격을 시뮬레이션하고 지연 시간과 패킷 손실을 모델링할 수 있습니다. 우리는 이 모델을 "Inferred model"이라고 부르며, 이외에도 AS의 연결성에 따라 구성된 간단한 모델 두 가지를 시험했습니다. Nyx가 간단한 모델과 함께 효과적으로 작동하는 것을 IV-B6 절에서 보여줄 것입니다.

인터넷 상의 트래픽 흐름을 모델링하기 위해서는 트래픽이 어디에서 발생하고, 어디로 향하는지, 그리고 얼마나 많은지를 알아야 합니다. 우리는 기존 연구, 특히 Gill 등의 연구 [28]와 Labovitz 등의 측정 [29], 세계 은행 [30], PeeringDB [31], 그리고 Sandvine [32]의 지원을 기반으로 모델을 구축했습니다. Sandvine은 다양

한 지역의 "평균" 사용자로부터 대역폭 소비량을 제공합니다. 이 정보는 세계 은행의 각 국가별 인터넷 사용자 수 추정치와 결합되어 국가별 상대적인 수신 및 발신 대역폭을 얻을 수 있었습니다. 이 대역폭을 AS에 할당하기 위해, 우리는 먼저 각 AS를 주로 속한 국가로 할당했고, 이를 위해 IANA의 할당된 AS 번호 [33]를 사용했습니다. 그런 다음 AS들이 다른 AS들과 피어링할 의사를 공개하는 시스템인 PeeringDB를 참고했고, 이 시스템은 AS들이 처리하는 평균 수신 및 발신 트래픽 양도 제공합니다. 인터넷에 약 58,000개의 AS가 있지만, 이 데이터셋에는 약 8,000개 이상의 대역폭 추정치 보고가 있습니다.

모든 AS 간의 상대적 대역폭 값을 설정하기 위해 Scikit-Learn [34]을 사용하여 결정 트리 분류기를 학습했습니다. 위에서 설명한 데이터와 AS의 특성(AS 차수, AS 고객 콘 크기, AS의 주요 운영 국가, AS가 광고하는 IP 공간의 크기 등)을 기반으로 학습되었습니다. 결과적으로 얻은 분류기는 약 10% 미만의 오분류 오차를 가지며, 사용 가능한 모든 데이터를 사용하여 대략 90%의 정확도를 가진 추정 모델이라는 것을 보여줍니다.

한편, 우리의 추정 대역폭 모델이 완벽하지 않다는 점을 인식하고 있습니다. 그러나 현재 인터넷 전체의 트래픽 수준을 완전히 근사화할 충분한 대역폭 모델을 수립한 문헌은 없습니다. 사용된 모델에 관계없이, 시뮬레이터 내의 링크 대역폭은 배포 AS나 Nyx에게 절대로 공개되지 않으며, 평가를 위해 시뮬레이터에서만 사용됩니다.

1. 봇넷 모델: 네트워크 토폴로지와 함께 봇 배치는 시뮬레이션 결과에 영향을 줄 수 있습니다. 이 논문에서는 세 가지 봇넷 데이터셋을 사용합니다. 최근 봇넷 IP를 열거하는 연구가 진행되었고, 우리는 이를 의존합니다. 첫 번째 데이터셋은 2016년부터 2017년까지 관찰된 2,900,000개의 고유한 Mirai 호스트로 구성됩니다 [35]. Mirai는 최근에 Dyn과 Liberia와 같은 기관에 대한 트랜짓 링크 공격을 모델링하기에 이상적인 분포를 나타냅니다 [19], [2] 그리고 대부분의 경우 IoT 기기에 집중되어 있습니다. 두 번째 봇넷은 2012년부터 2013년까지 관찰된 총 2,800,000개의 고유한 호스트로 구성된 23개 봇넷 패밀리인 Conficker 봇넷입니다 [36]. Mirai와 Conficker 봇넷 모두 상대적으로 적은 수의 AS에 집중되어 있으며, 부록의 그림 12에서 볼 수 있듯이 AS의 97% 이상에서 50개 미만의 봇이 있습니다. 각 봇의 IP 주소는 CIDRS와 연관시켜 부모 AS에 매핑되었으며, CIDRS를 ASN에 묶기 위해 RouteViews 데이터 [37]를 사용했습니다. 이를 통해 AS당 대략적인 봇 수를 계산할 수 있습니다.

더 분산된 봇넷을 사용하는 적 대처를 위해 우리의 세 번째 및 마지막 데이터셋은 배포형 봇넷입니다. 이 봇넷은 배포형 봇 AS로 이루어진 전체적으로 분산된 형태로 구성되어 있으며, 배포된 AS 중에서는 deployer와 critical AS를 제외하고 모두 악성 트래픽을 전송할 수 있습니다.

4. 공격 시나리오: Nyx는 트랜짓 링크 DDoS와 전통적인 DDoS에 영향을 받을 때 deployer AS를 보호하려고 시도합니다. 전통적인 DDoS의 경우, deployer AS부터 시작하여 공격된 세그먼트에 대한 라우팅 성공을 측정합니다. 이 시나리오에서 봇은 deployer AS로 직접 트래픽을 보내는 것뿐만 아니라 deployer와 critical AS 사이의 각 호합 세그먼트로 보냅니다. 따라서 기본 프리 존에서 AS 세그먼트로의 긴 경로를 가진 봇 AS는 주어진 트랜짓 코어 AS와 달리 AS의 많은 수의 경로를 가지고 있지 않다는 점에 유의해야 합니다. 이후 이 섹션에서 보여줄 것처럼, 우리는 선택된 시나리오에 민감하지 않으며, 오늘날 가장 주요한 DDoS 공격 형태에 대해 방어할 수 있음을 보여줍니다.

5. 시뮬레이션 방법론: 우리의 이벤트 드리븐 네트워크 시뮬레이터는 Nyx의 효과를 평가할 수 있게 합니다. 시뮬레이션 시작 시, BGP 라우터는 동료와 연결되어 안정된 네트워크 상태를 형성합니다. 이 시뮬레이션 라우터들은 앞서 설명한 추론된 AS 관계 및 밸리프리 라우팅 정책을 사용합니다. 네트워크가 안정된 상태에 도달하면 시뮬레이터는 반복적으로 토폴로지에서 deployer와 critical AS를 선택하고, 현재 쌍에 대해 전통적인 DDoS와 트랜짓 링크 DDoS를 시뮬레이션합니다. 각 deployer-critical 쌍에 대해, 정상 트래픽 흐름은 IV-A2절에서 설명한 대역폭 모델을 사용하여 전체 토폴로지로 보내집니다. 그런 다음 시뮬레이터는 테스트되는 봇넷 모델에 따라 봇을 보유한 AS에서 봇을 끌어내어 deployer와 critical AS 사이의 최적 경로를 따라 각 링크를 반복적으로 혼잡시킵니다.

Nyx는 이후 Section III-B와 Section III-D에서 설명한 기술을 사용하여 장애가 있는 링크 주변에 들어오는 critical 트래픽을 대체 경로로 라우팅합니다. Nyx는 혼잡을 피하도록 라우팅하기 전후에 시뮬레이터가 deployer에서의 패킷 손실 성능을 측정하며, 이는 구독 요소로 표시됩니다. 이 값은 0.0에서 5.0 사이이며, 1.0은 각 링크가 수용 능력에 도달한 것을 나타내며, 더 많거나 덜하면 수용 능력을 초과하거나 미달함을 의미합니다. 시뮬레이터는 혼잡 요소를 통해 혼잡을 측정하며, 이는 시뮬레이션에서 2.0 또는 5.0 중 하나이며, 시뮬레이터는 링크를 혼잡하게 만들기 위해 충분한 봇 트래픽을 보냅니다. 이렇게 함으로써 혼잡 요소는 공격의 강도를 결정합니다. 두 번째 요인은 대역폭 허용량으로 모델링됩니다. 대역폭 허용량은 1.0에서 2.0 사이의 상수 값으로, 정상 용량이 1.0인 경우 각 링크가 추가 트래픽을 처리할 수 있는 정도를 설명합니다. 예를 들어, 대역폭 허용량이 1.5인 경우 AS는 정상 용량의 50% 더 많은 트래픽을 처리할 수 있으며, 1.0보다 높은 경우 링크가 혼잡하여 흐르는 트래픽을 끊을 수 있습니다. 시뮬레이터는 원래 최적 경로 및 대체 경로를 따라 각 링크의 구독 요소를 측정하고, 새 경로의 최악의 구독 요소를 결정하여 Nyx가 혼잡을 피하는 데 효과적으로 얼마나 성공했는지 평가합니다.Nyx는 이 평가 프로세스를 모든 대역폭 모델, 봇넷 모델, 공격 시나리오, 공격 강도 설정에 대해 따릅니다. 이러한 시뮬레이션을 통해 이 섹션 초반에서 설명한 질문에 대답할 수 있습니다. Nyx의 혼잡을 피하고 대체 경로로 라우팅하는 능력을 라우팅 성공이라고 합니다. Nyx가 Section IV-B2에서 설명한 경로 라이닝 기술을 사용하여 장애를 완화하는 능력을 장애 완화라고 합니다. 모든 링크가 완전히 혼잡하지 않은 대체 경로로 혼잡을 피하고 critical 트래픽을 라우팅하여 구독 요소가 1.0 미만인 강력한 성능 성공이라고 합니다. 마지막으로, Nyx가 모든 작업을 수행하면서 경로를 더 길게 라우팅하지 않는지도 탐구합니다.

B. 시뮬레이션 결과저희 시뮬레이터를 통해 Nyx는 다양한 대역폭 모델과 공격 강도 파라미터에 따라 봇넷을 제어하는 적대적 요소에 대해 테스트되었으며, 트랜짓 링크 및 전통적인 DDoS 시나리오에 대해 테스트되었습니다.

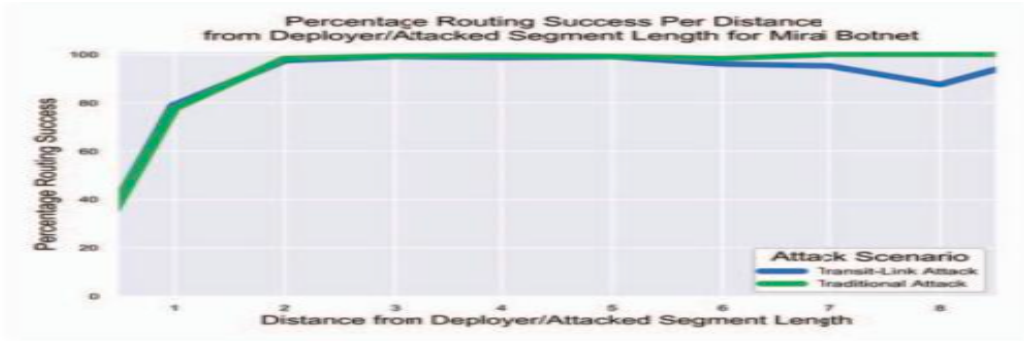
1) Nyx는 DDoS 공격에 영향을 받지 않은 링크로 트래픽을 이동할 수 있습니까?:

Nyx는 유효한 경로를 찾고, 거의 완벽한 성공률로 혼잡한 링크 주변의 들어오는 트래픽을 이동시킬 수 있습니다. 이는 현재 시스템이 실패하는 거대한 트랜짓 링크 및 전통적인 DDoS를 완화하기 위한 첫 번째 단계입니다. 저희 시뮬레이터는 Nyx를 두 가지 유형의 DDoS 시나리오에 대해 라우팅 성공을 평가하고, 이 결과를 라우팅 성공으로 라벨링합니다.

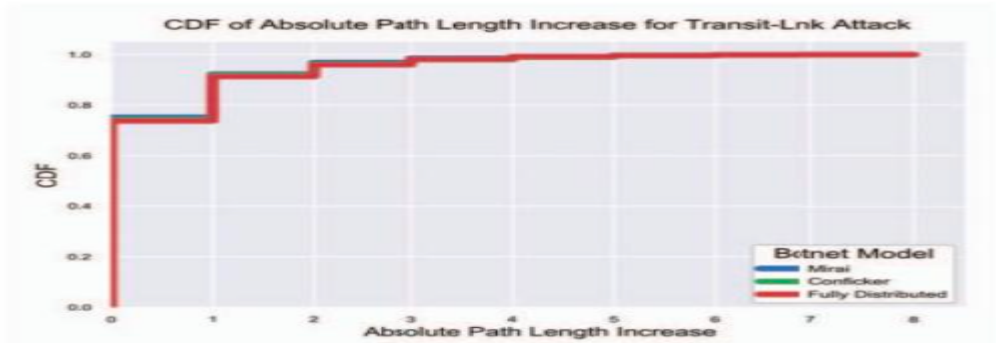
Figure 5에서 보듯이, 저희 시스템은 deployer로부터 2에서 8개의 호프 사이에 있는 AS들의 들어오는 트래픽에 영향을 미치기 위해 FRRP를 사용할 때 거의 100%의 라우팅 성공률을 달성했습니다. 이는 deployer AS 상위의 트랜짓 링크가 공격을 받을 때, deployer AS가 선택한 critical AS의 들어오는 트래픽을 영향을 받는 링크를 피하도록 성공적으로 이동시킬 수 있다는 것을 의미합니다.

공격이 트랜짓 링크에 집중될 때 뿐만 아니라 전통적인 DDoS 공격에도 들어오는 트래픽을 높은 성공률로 라우팅할 수 있습니다. 전통적인 DDoS 공격에서는 deployer로부터 1호프 이상의 링크로 이동하는 경우에는 78% 이상의 성공률을 보였으며, deployer 자체에서 2호프 이상 떨어진 링크로 트래픽을 이동하는 경우에는 거의 100%에 가까운 성공률을 보였습니다. 이는 공격하는 봇넷이 deployer로부터 critical AS로 이르는 경로 상의 deployer에 가장 가까운 두 링크를 공격할 때, deployer가 해당 critical AS의 트래픽을 거의 100% 성공률로 영향을 받는 두 링크를 피하도록 트래픽을 이동시킬 수 있다는 것을 의미합니다.

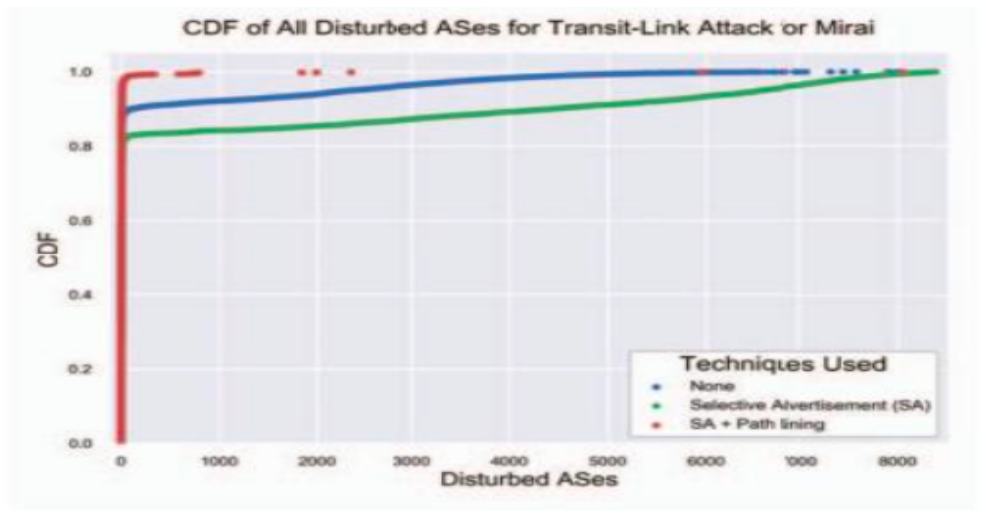
부록의 Figure 14에서 우리는 Conficker 모델에서 혼잡을 피하고 대안적인 경로로 라우팅할 수 있음을 보여줍니다. 이 경우, deployer로부터 2에서 8호프 사이의 라우팅 성공률은 98% 이상입니다. 이는 상위 트랜짓 링크가 공격을 받을 때와 deployer 자체가 직접 공격을 받을 때 모두 해당됩니다. 마지막으로 부록의 Figure 15에서 전 세계적으로 분산된 봇넷에 대한 공격을 받을 때, Nyx는 거의 100%의 성공률로 critical AS로부터 들어오는 트래픽을 이동시킬 수 있음을 보여줍니다. 이는 deployer와 critical AS를 제외한 모든 AS가 deployer로 직접 공격 트래픽을 보내거나 상위 링크로 공격 트래픽을 보낼 때에도 다른 경로로 들어오는 트래픽을 조정할 수 있음을 보여줍니다.



[그림 14] Fig. 5: Mirai 사용한 트랜짓 링크 공격 시나리오의 라우팅 성공률 백분율



[그림 15] Fig. 6: Mirai를 사용한 트랜짓 링크 공격 시나리오에서의 절대적인 경로 길이 증가



[그림 16] Fig. 7: Mirai를 사용한 트랜짓 링크 공격 시나리오에서 교란된 AS 수

모델링된 지연: 교란 완화에 대한 토론 이전에 시뮬레이터가 Nyx의 지연에 미치는 영향을 평가하는 방법에 대해 먼저 알아봅니다. 대규모 분산 시스템의 지연을 모델링하는 것은 매우 어려운 것으로 받아들여지고 있습니다. 따라서 우리는 경로 길이를 지연의 대리 측정 항목으로 사용하는 일반적인 개념을 채택합니다. 실제로, 인터넷에서 선택한 대체 경로의 지연 시간을 측정하는 것은 AS 간 물리적 케이블과 AS 간 지리적 거리, 그리고 BGP 데몬을 실행하는 하드웨어의 품질과 같은 1계층 기술에 많이 의존합니다.

DDoS를 피하면 대체 경로의 경로 길이가 5개 이상의 홉 증가가 발생하는 경우는

전체 실행의 2%에 불과하며, 94%의 경우에는 경로 길이 증가가 없다는 것이 확인되었습니다. 이는 트랜짓 링크 DDoS에 대한 Figure 6에서 보여지는 것입니다. 전통적인 DDoS의 경우 Figure 16에 거의 동일한 결과가 나타납니다. Figure 6는 또한 Conficker 및 전체 분산 봇넷 모델을 사용할 때의 경로 길이 증가를 보여줍니다. 이러한 결과는 거의 94% 이상의 경우에 경로 길이 증가가 없다는 것을 보여주며, 이는 Nyx가 봇넷 모델의 변경에 대해서도 경로 길이 증가에 둔감하다는 것을 보여줍니다. 전체적인 네트워크 혼잡이 새로운 경로에서 실제로 개선되었는지 여부와 관계없이 경로 길이 증가에 관계없이 경로 성공을 달성할 수 있으며, 네트워크 혼잡이 새 경로에서 완화된 경우 경로 성공은 IV-B3절에서 자세히 다룹니다. 다음 섹션에서는 III절에서 설명한 두 번째 도전 과제인 교란 완화를 어떻게 다루는지에 대해 논의하겠습니다.

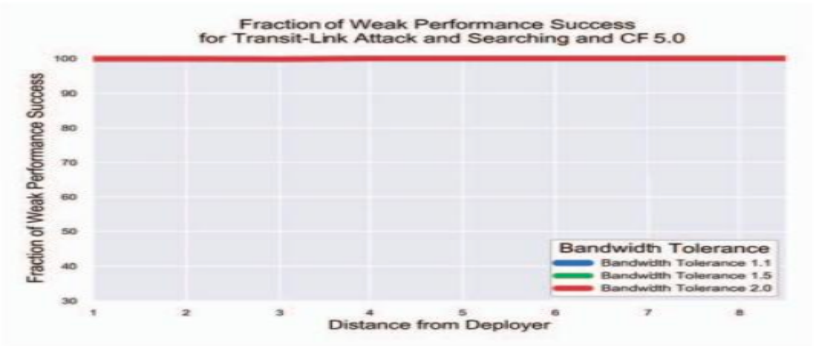
2) 다른 AS에게 교란을 주지 않고 Nyx가 트래픽을 이동할 수 있는가?: 주요 DDoS 공격의 영향을 받지 않는 새로운 경로로 들어오는 트래픽을 성공적으로 이동할 수 있었지만, Nyx가 사용하는 FRRP 기술이 상당 수의 AS를 교란시켰습니다. 교란 문제를 극복하기 위해 우리는 섹션 III-C에서 Nyx가 사용할 두 가지 전략을 도입했습니다: 선택적 광고와 경로 정렬. 이러한 전략을 함께 사용할 때 Nyx는 들어오는 트래픽을 이동할 때 배치하는 AS 주변의 교란을 크게 줄였습니다.

트랜짓 링크 DDoS의 경우, 교란을 완화하기 위한 전략을 적용하기 전에는 Nyx가 대부분의 시간에 1,000에서 6,000개의 AS를 교란시켰습니다. 이는 현대 인터넷에서 모든 AS의 약 10%에 해당합니다. 이는 트랜짓 링크 DDoS 또는 전통적인 DDoS 공격 시나리오에 있어서도 마찬가지입니다. Figure 7에서는 Mirai 봇넷 모델의 트랜짓 링크 DDoS 시나리오만 보여줍니다. 전통적인 DDoS 및 다른 봇넷 모델은 부록의 Figure 17에서 확인할 수 있습니다.

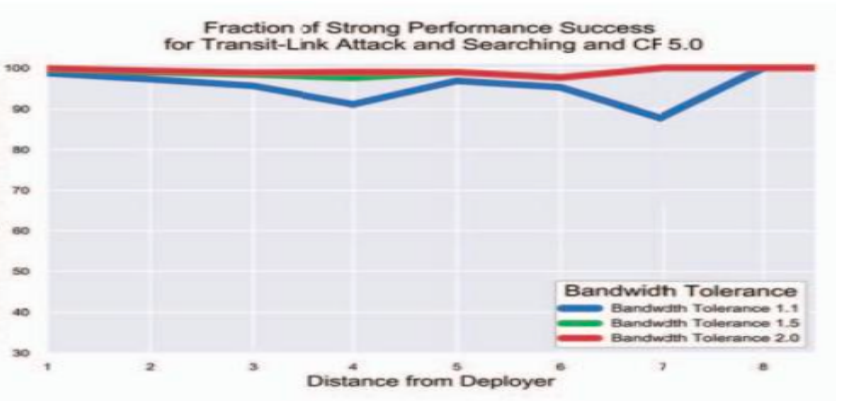
그러나 Nyx가 채택한 교란 완화 전략은 봇넷 모델이나 공격 시나리오와는 상관없이 매우 효과적입니다. 선택적 광고만 사용했을 때는 교란이 줄지 않았지만, 경로 정렬과 결합하면 교란된 AS의 수가 평균적으로 5,000개에서 평균적으로 10개 미만으로 감소했습니다. 교란이 줄어듦에 따라 Nyx는 트랜짓 링크가 공격받을 때와 배치 AS가 직접 공격받을 때의 배포 비용을 줄였습니다. 또한 이러한 AS 각각에 대해 Nyx는 모든 봇넷에 대해 해당 AS에 거주하는 IP의 수가 100개 미만인 교란을 유발했습니다. 이러한 결과는 여기에는 표시되지 않았습니다.

로컬 선호도 변경사항이 있나요?: AS의 최적 경로나 배포 AS의 채택한 경로 길이 외에도, 우리는 한 제공업체에서 다른 제공업체로의 링크 사용에 따른 비용 문제를 해결했습니다. 현대 인터넷에서 한 링크를 다른 링크로 전환하는 실제 비용은 엄격하게 보호되는 비밀입니다. 따라서 우리는 동료 또는 제공업체 학습 경로로 전환하는 행위를 추가적인 비용의 대리자로 사용했습니다. 시뮬레이션에서 Nyx를 사용하는 배포 AS는 고객 학습 경로에서 동료 또는 제공업체 학습 경로로 전환하지 않습니다. 우리는 현재 이러한 행동을 더 많은 시뮬레이션을 통해 설명하고 있습니다.

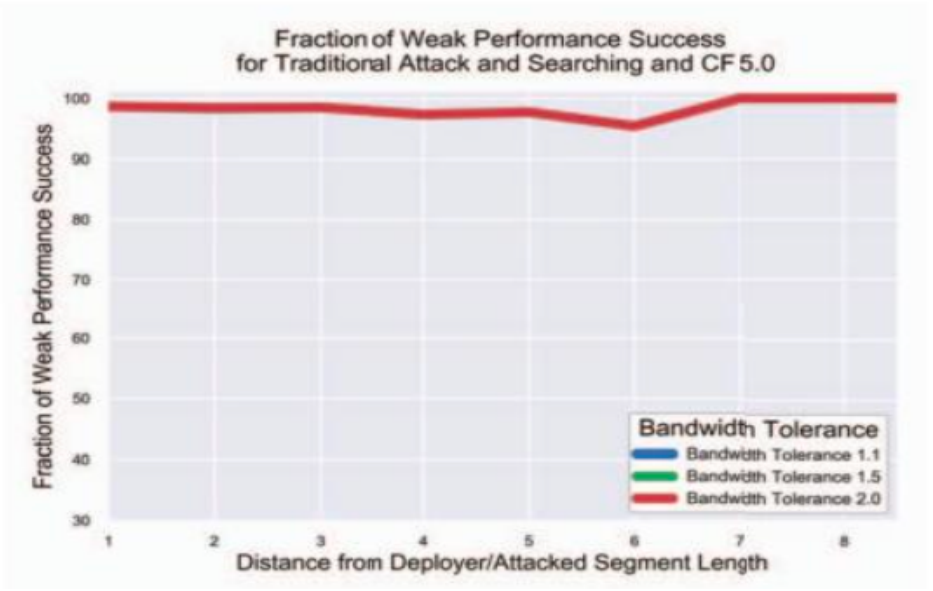
3) 대체 경로에 충분한 용량이 있나요?: Nyx가 들어오는 트래픽을 성공적으로 이동할 수 있고 거의 교란이나 전혀 없이 이동할 수 있음을 보여준 지금, 우리는 Nyx가 거의 모든 경우에 트랜짓 링크 DDoS 및 전통적인 DDoS의 대부분 경우에 혼잡한 경로를 우회하여 혼잡하지 않은 경로로 성공적으로 이동할 수 있다는 것을 보여줍니다. 성능 좋은 경로를 측정하기 위해 대역폭 허용치 (1.1, 1.5, 2.0) 및 혼잡 요소를 사용합니다.



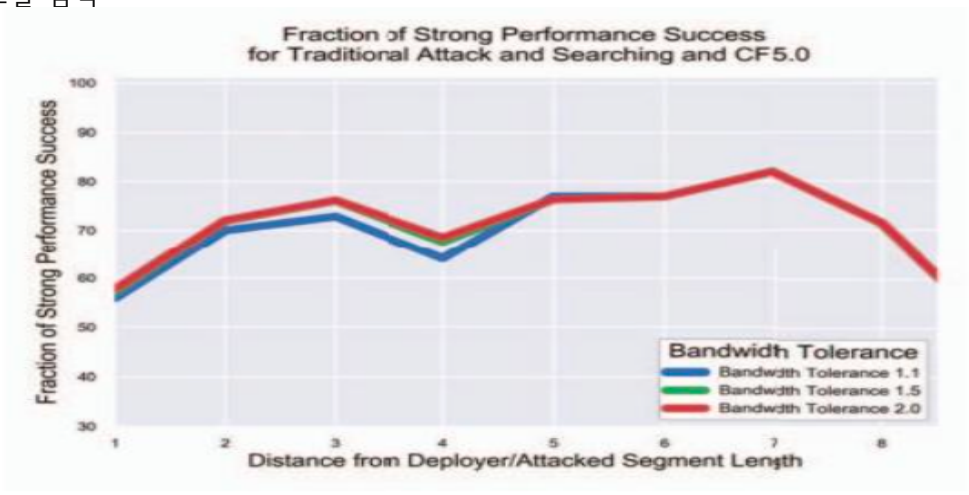
[그림 17] (a) 트랜짓 링크 DDoS에 대한 약한 성능 성공 - Mirai 및 추론된 대역폭 모델 검색



[그림 18] (b) 트랜짓 링크 DDoS에 대한 강한 성능 성공 - Mirai 및 추론된 대역폭 모델 검색



[그림 19] (c) 전통적인 DDoS에 대한 약한 성능 성공 - Mirai 및 추론된 대역폭 모델 검색



[그림 20] (d) 전통적인 DDoS에 대한 강한 성능 성공 - Mirai 및 추론된 대역폭 모델 검색

그림 8: 트랜짓 링크 및 전통적인 DDoS 공격 시나리오에 대한 성능 성공 지표

==========

그림 8a에서 보여지는 것처럼, 배포 AS는 Nyx를 사용하여 검색을 통해 트랜짓 링크 DDoS의 경우 거의 100%의 비율로 약한 성능 성공을 달성할 수 있습니다. 이는 어떤 트랜짓 링크가 공격을 받더라도 우리는 거의 100%의 경우에서 혼잡을 어느 정도 완화할 수 있다는 것을 의미합니다. 그러나 모든 혼잡을 완전히 해소할 수 있는지는 어떨까요? 그것을 그림 8b에서 다시 검색과 함께 보여줍니다. 여기서 원래의 용량보다 5배나 혼잡한 상황에서 95% 이상의 경우에 성능 좋은 경로를 찾아내는 것을 확인할 수 있습니다. 우리가 검색을 사용하지 않을 때는 부록의 그림 18b에서 보듯이, 경우에 따라서는 대략 89%의 케이스에서 성공을 볼 수 있습니다. 이러한 결과는 대역폭 허용 한계와 혼잡 요소의 가장 어려운 설정을 대상으로 한 것으로, Nyx가 극도로 열악한 조건에서도 혼잡을 피해 경로를 찾을 수 있는 능력을 보여줍니다. 또한, 외부 협력 없이도 가능합니다.

트랜짓 링크 DDoS 공격을 받을 때 배포 AS를 보호할 수 있을 뿐만 아니라, 대역폭 허용 한계와 혼잡 요소의 가장 어려운 설정에 대해 배포 AS를 직접적으로 대상으로 공격받을 때도 보호할 수 있다는 것을 보여줍니다. 그림 8c에서 보여지는 것처럼, 우리는 평균적으로 93%의 경우에 원래 경로보다 성능이 더 좋은 링크로 트래픽을 이주시킬 수 있습니다. 강한 성능 성공의 경우에는 평균적으로 75%의 경우에 완전히 혼잡하지 않은 경로로 트래픽을 이주시킬 수 있습니다. 검색을 사용할 때 약한 성능 성공률이 높아지는 것을 그림 8c에서 볼 수 있지만, 강한 성능 성공에 대해서는 그림 8d에서 볼 수 있듯이 검색이 큰 도움이 되지 않는 경우도 있습니다.

전통적인 DDoS가 보호하기 어려운 케이스인 이유는 무엇일까요? 답은 Nyx가 FRRP를 어떻게 활용하는지에 있습니다. 전통적인 DDoS 공격을 받으면 배포 AS에서 홀 펀칭된 경로를 광고하게 되는데, 이 경우에는 배포 AS로 직접 주소지정된 대량의 봇 트래픽을 끌어오게 될 수 있습니다. 반면 트랜짓 링크 DDoS의 경우 봇 트래픽은 배포 AS를 대상으로 주소지정되지 않습니다. 이 경우 봇 트래픽은 배포 AS로 끌어오지 않게 됩니다. 이러한 부작용에도 불구하고, 우리는 미리 알려진 중요 AS로부터의 중요 트래픽을 상당 부분 보호할 수 있는 시스템을 증명했으며, 기존의 DDoS 방어 방법을 사용하여 인프라 기반 공격에 대해 어떤 경우에도 수행할 수 없는 경우도 있습니다.

또한 시뮬레이션 결과는 우리 시스템이 검색을 활용할 때, 배포 AS로부터 더 멀리 떨어진 경우를 제외하고는 검색하는 깊이가 작음을 보여줍니다. 부록의 그림 13에서 설명된 것처럼, 이는 배포 AS가 Nyx를 구현하는 BGP 스피커들에게 영향을 받은 링크 주변의 성능 좋은 경로를 찾기 위해 소중한 시간을 낭비시킬 필요가 없다는 것을 의미합니다. 트랜짓 링크 DDoS의 경우 평균적으로 거의 0회의 반복에서 수행되며, 배포 AS로부터 8홉 이상 떨어진 경우에는 최악의 경우 평균적으로 14회의 반복에서 수행됩니다.

이러한 결과를 통해, 우리는 Nyx를 사용하여 전통적인 DDoS 공격을 받을 때에도, 배포 AS로부터 알려진 중요 AS로 들어오는 트래픽을 DDoS에 영향을 받지 않는 링크로 평균적으로 75%의 시간 동안 이주시킬 수 있다는 것을 입증합니다. 또한, 기존 작업과는 달리 배포 AS는 외부 협력 없이도 Nyx를 활용할 수 있습니다.

4) Nyx는 공격 강도에 무감인가요?: 대역폭 허용 한계와 혼잡 요소의 경우 성능 성공에 대해 결과를 논의했지만, 이러한 값들이 우리 시스템의 성공을 보장하기 위해 단순히 선택된 값인지 어떻게 보여줄 수 있을까요? 우리는 그림 9에서 보여줍니다. Mirai 봇넷 모델에 대해, 대역폭 허용 한계가 1.1 이상인 경우에는 허용 한계를 더 높여도 얻는 이득이 안정화되고 더 이상 증가하지 않습니다. 이는

DDoS 공격 주변의 링크 용량에 얼마나 많은 여유를 주든 강한 성능 성공이 증가하지 않는다는 것을 나타냅니다. 따라서 시뮬레이션에서 선택한 값들은 우리가 더 큰 성공을 보장하기 위해 설정된 것이 아닙니다.

혼잡 요소의 경우, 우리는 다른 테스트된 요소인 2.0과 같은 작은 혼잡 요소에 대해 약간 더 높은 성능 성공만을 보입니다. 그러나 그 차이는 크지 않습니다. 여기에는 나와 있지 않지만, 작은 혼잡 요소 2.0은 강한 성능 성공에 큰 영향을 미치지 않으며, 평균적으로 추가로 성공적인 경우가 5% 미만으로 나타납니다. 이는 트랜짓 링크가 공격을 받거나 배포 AS가 직접 공격을 받을 때의 경우 모두 해당됩니다. 이러한 결과를 고려할 때, 우리 시뮬레이션에서 선택한 혼잡 요소 값은 공격자가 배포 AS와 중요 AS 간의 정상 경로의 링크를 계속 혼잡하게 만들 수 있고 Nyx가 여전히 영향을 받은 링크를 우회하고 혼잡을 완화할 수 있다는 것을 나타냅니다.

5) Nyx는 봇넷 모델에 무감인가요?: IV-A3에서 우리는 세 가지 봇넷 모델인 Mirai, Conficker 및 완전 분산형 봇넷을 설명했습니다. 이전 섹션에서는 Nyx가 Mirai와 유사한 크기와 토폴로지를 가진 봇넷을 제어하는 경우 전통적인 DDoS의 효과를 크게 완화시키고, 트랜짓 링크 DDoS로 인한 혼잡을 거의 제거한다는 것을 보여주었습니다. 그러나 Nyx는 Conficker와 같은 다른 모델에서도 잘 작동하며, 부록의 그림 12에서 확인할 수 있습니다. Conficker의 경우 Mirai와 유사한 분포와 카디널리티를 가지고 있습니다. 완전 분산형 봇넷의 경우, Nyx는 대역폭 허용 한계와 혼잡 요소의 가장 어려운 설정에 대해 트랜짓 링크 DDoS의 경우 평균적으로 99%의 강한 성능 성공을 달성합니다. 전통적인 DDoS의 경우, 부록의 그림 20에서 확인할 수 있듯이 평균적으로 78%의 강한 성능 성공을 달성합니다.

이는 현대 인터넷의 거의 모든 AS가 명령에 따라 공격 트래픽을 보낼 수 있는 봇을 보유한 전 세계적으로 분산된 공격자가 다른 AS의 외부 협력 없이도 Nyx를 사용하여 DDoS 이벤트를 우회할 수 있다는 것을 의미합니다.

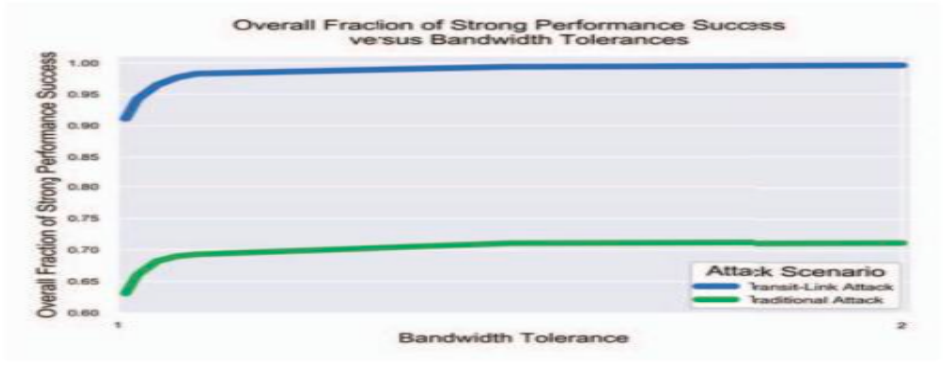
6) Nyx는 대역폭 모델의 선택에 무감인가요?: IV-A2에서는 시뮬레이터에서 사용하는 주요 대역폭 모델에 대해 설명했습니다. 이 모델은 꽤 복잡하지만, 다양한 신뢰할 수 있는 데이터 소스를 사용하여 기존 AS를 통한 전형적인 트래픽 수준을 근사화합니다. 이제 간단한 모델로 시스템의 성능을 평가하고, Nyx가 인터넷의 링크 용량 선택에 무감함을 보여줍니다. 선택한 추가 모델은 AS Degree 및 각 AS 내의 총 IP 수에 기반했습니다.

그림 10과 11은 우리 시스템이 테스트된 모든 대역폭 모델에 대해 거의 동일한 강한 성능 성공률을 달성한다는 것을 보여줍니다. 가장 복잡하고 일반적인 추론된 모델이 혼잡 완화 측면에서 전반적으로 가장 나쁜 성능을 보이고 있습니다. 트랜짓 링크 공격 시나리오에서 우리 모델들은 평균적으로 약 95%의 강한 성능 성공률을 보이며, 전통적인 공격 시나리오에서는 평균적으로 약 70%에서 75%의 성공률을 보입니다. 따라서 인터넷의 링크 용량을 AS Degree 및 AS Total IP 수의 함수로 모델링함으로써 Nyx는 보다 복잡한 대역폭 모델과 유사한 결과를 달성할 수 있습니다.

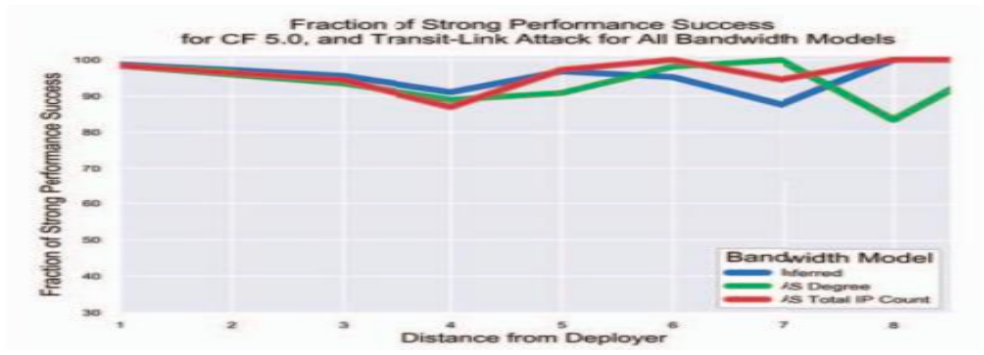
V. 관련 연구

전통적 및 현재의 DDoS 방어 시스템은 다양한 방법을 통해 피해자에서의 패킷 손실과 증가된 지연을 완화하려고 시도합니다. 그러나 Nyx가 사용하는 루트 변경 기술을 통한 DDoS 방어 시스템은 존재하지 않습니다. 이 섹션에서는 최근 문헌에서 여러 유형의 DDoS 방어 시스템을 논의한 후, 이러한 시스템이 최근의 트랜짓 링크 DDoS 공격과 Mirai와 같은 봇넷을 활용한 대규모 전통적 DDoS 공격으로부터 보호하지 못하는 이유를 논의할 것입니다. 또한 왜 우리 시스템이 이러한 기존 시스템과 동일한 결함을 겪지 않는지에 대해 논의할 것입니다.

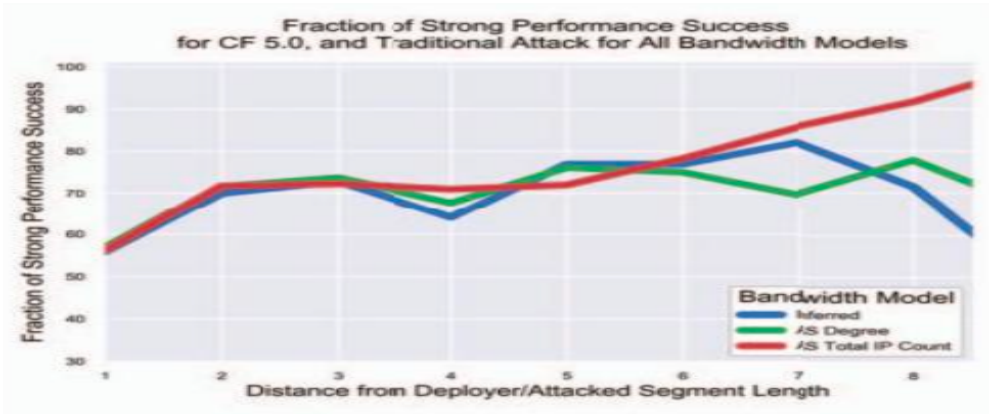
전통적인 DDoS 방어 시스템은 패킷 필터링을 통해 DDoS 공격을 완화하려고 시도합니다. 패킷 마킹 및 푸시백 기술과 같은 기법을 사용하여 네트워크의 입구 출구 지점에서 트래픽을 필터링하지만, 우리 평가에서 사용된 Mirai 봇넷과 같은 규모의 DDoS 공격에 대한 대응력이 부족합니다. 일반적으로, 최소한의 배치 요구사항을 갖춘 기존 시스템은 봇넷 크기에 독립적이며, 악의적인 봇넷의 공격 트래픽 크기에 관계없이 공격에 대처할 수 있는 능력을 제공하지 않습니다. 대규모 봇넷에 대한 방어 이외에도, 트랜짓 링크 DDoS는 공격 트래픽을 피해자 AS로 직접 보내지 않고 상류 링크 또는 인터넷의 원하는 위치로 보내므로, 공격 트래픽을 필터링하는 것은 불가능합니다. Nyx는 분산된 봇넷에서 보내는 대규모 수신 트래픽을 처리할 수 있습니다. 왜냐하면 트랜짓 링크 공격의 경우 악성 트래픽을 물리적으로 처리할 필요가 없을 뿐 아니라 중요한 트래픽이 취해지는 경로를 임의로 변경하여 혼잡한 링크를 우회할 수 있기 때문입니다. 이렇게 함으로써 피해자 AS의 상류 링크에 공격 트래픽을 분산시킬 수 있습니다.



[그림 21] Fig. 9: 다양한 대역폭 허용 한계에 대한 트랜짓 링크 공격 시나리오에서의 강한 성능 성공률



[그림 22] Fig. 10: 모든 대역폭 모델에 대한 트랜짓 링크 공격 시나리오에서의 강한 성능 성공률



[그림 23] Fig. 11: 모든 대역폭 모델에 대한 전통적인 공격 시나리오에서의 강한 성능 성공률

특정 서비스(예: HTTP 또는 DNS)를 대상으로 하는 트래픽을 필터링하는 기술 [43], [44], [45]은 다른 서비스나 심지어 기저 제어 평면을 공격하는 DDoS 공격에 대해 비효과적입니다. 인터넷 네트워크 트래픽은 모두 BGP 라우터에 의해 결정된 경로를 통해 전송되어야 하기 때문에, Nyx는 광고된 경로를 반응적으로 변경하여 공격자가 전송하는 트래픽의 유형에 관계없이 피해자 AS가 알려진 중요 AS에서의 트래픽을 악성 트래픽에 영향을 받지 않는 경로로 이동시킬 수 있습니다.

게임 이론적 접근 방식을 사용하는 전략은 방어자의 최적 전략을 모델링하여 공격자의 비용을 최대화하는 데 초점을 맞춥니다 [46], [47], 그러나 이러한 접근 방식은 클릭 한 번으로 대규모 DDoS 공격을 쉽게 시작할 수 있는 현재 상황에서는 효과적이지 않습니다. Zhou 등의 연구는 인터넷의 백본 및 고도로 연결된 AS를 보호하기 위한 시스템을 모델링했지만 [48], 트랜짓 링크 DDoS에 대한 방어는 실패했습니다. 왜냐하면 제안된 시스템은 피해자 AS 내에서 배포된 시스템에 도달한 후에만 트래픽을 처리하기 때문입니다. 다른 최근 연구들은 이와 같은 배포 방식을 채택하여 피해자 AS에서 통계적 방법을 사용하여 봇넷 트래픽을 감지하고 모델링하려고 시도하지만 [49], [50], 트랜짓 링크 DDoS의 경우 이러한 접근 방식은 불가능합니다.

VI. 결론

본 논문에서는 트랜짓 링크 DDoS의 영향을 크게 줄일 수 있는 새로운 시스템인 Nyx를 제안했습니다. 이는 이전에 해결되지 않은 형태의 DDoS로 전체 국가를 허물어놓는 데 사용되고 있으며 전통적인 DDoS에도 효과적입니다. 더 중요한 점은 Nyx가 피해자 AS의 경계에만 배치되면 되며 다른 AS들로부터의 협력이 필요하지 않아 수신 트래픽의 품질을 보장할 수 있습니다. 먼저, Nyx를 배치하는 AS(배포 AS라고 함)가 AS에서 나가는 트래픽뿐만 아니라 들어오는 트래픽 경로도 조작할 수 있다는 것을 보였습니다. 이 능력은 우리 시스템이 배포자가 항상 트래픽이 도달하기를 원하는 선택된 중요 AS에서 나오는 트래픽을 DDoS 공격에 영향을 받는 링크를 우회하여 거의 100%의 성공률로 처리할 수 있게 합니다. 둘째, Nyx가 영향을 받는 링크 주변에서 들어오는 중요한 트래픽을 이동시키면서 우리 시스템을 사용하는 AS와 근접한 많은 수의 AS를 방해하지 않는 것을 보였습니다. 우리의 기술을 사용하기 전에는 평균적으로 1000~5000개의 AS가 방해되었지만, 이제는 평균적으로 10개 이하의 AS만이 방해됩니다. 세 번째로, 우리는 Nyx가 DDoS 공격 시나리오와 관계없이 98% 이상의 경우에 영향을 받는 링크에서 트래픽을 다른 링크로 이주시킬 수 있음을 입증했으며, 트랜짓 링크 DDoS의 경우 98% 이상의 성공률로 완전히 혼잡하지 않은 경로로 이동시킬 수 있으며, 전통적인 DDoS의 경우 평균적으로 75%의 성공률을 보여줍니다. 이로써 인터넷의 트랜짓 코어에 대규모 공격을 받을 때도 중요한 AS에서의 트래픽이 끊기지 않습니다. 결국, 이 연구는 최근 DDoS 공격에 실패한 비효율적인 필터링 및 우선 순위 설정 방법에 대한 현실적으로 배포 가능하고 입증된 성공적인 대안을 제시하고 있습니다. 더 나아가, 우리는 SCION 및 SIBRA에서 탐구한 대역폭 보장을 위해 인터넷 백본을 재설계할 필요 없이 Crossfire 및 CoremeIt와 같은 트랜짓 링크 공격에 대한 첫 번째 확장 가능하고 쉽게 배포 가능한 솔루션을 제공했습니다.

향후 연구우리가 개발한 시스템은 미래의 연구에 많은 흥미로운 기회를 제공합니다. 현재 우리 시스템은 단일 선택된 중요 AS에서의 트래픽을 보호하는 데만 사용됩니다. 그러나 네트워크 혼잡으로부터 여러 중요 AS에서의 트래픽을 보호하는 것이 일반적으로 필요할 수 있습니다. 둘째로, 우리의 적대적 모델은 라우팅을 고려하는 글로벌적인 적이 없습니다. 방어자가 국가 또는 주요 ISP 그룹과 같은 중요한 AS의 상당 부분을 제어하는 적에 대비하기 위해서는 이 적대적 모델이 중요해집니다. 마지막으로, 여러 배포자가 있는 경우 우리 시스템의 효과성을 활발히 연구하고 있습니다.