BGP 기반 DDoS 방어 서비스의 동작 이해

토니 미우 퉁[1], 첸수 왕2[,3(✉)], 진허 왕[2]

[1] 넥서스가드 주식회사, 첸완, 홍콩
[2] 시안교통대학교 소프트웨어 공학부, 시안, 중국
cxwang@mail.xjtu.edu.cn
[3] 중국 시안 자오퉁 대학교, 시안 710049, 시안 INNS 핵심 연구소

요약. 분산 서비스 거부 공격은 수십 년 동안 인터넷이 직면한 가장 어려운 과제 중 하나였습니다. 최근에는 피해자에 대한 방대한 악성 트래픽을 저렴한 네트워크로 우회하여 대규모 DDoS 공격을 완화하는 DDoS 방어 서비스(DPS)가 부상하고 있습니다. 한 가지 일반적인 접근 방식은 BGP 정책을 변경하여 트래픽을 재라우팅하는 것인데, 이 경우 비정상적인 BGP 라우팅 동역학이 발생할 수 있습니다. 그러나 이러한 행동과 그 결과에 대해 알려진 바는 거의 없습니다. 이러한 공백을 메우기 위해 본 논문에서는 두 단계에 걸쳐 BGP 기반 DPS의 동작에 대한 첫 번째 연구를 수행합니다. 첫째, 실제 DDoS 이벤트를 특성화할 수 있는 데이터가 부족하기 때문에 머신 러닝 기반 접근 방식을 제안하여 DDoS 이벤트를 식별합니다. 둘째, 일반적인 DDoS 공격에 대한 DPS의 동작을 분석하기 위한 새로운 알고리즘을 설계합니다. 실제 DDoS 공격 사례 연구를 통해 공격을 완화하는 데 사용된 정책을 면밀히 분석하여 몇 가지 의미 있는 결과를 얻었습니다. 이 연구는 효과적인 DDoS 공격 방어 체계의 설계에 대해 조명합니다.

키워드: DDoS 공격 - BGP 트래픽 - DPS 동작

1 소개

분산 서비스 거부(DDoS) 공격은 수십 년 동안 인터넷 인프라를 위협해 왔습니다. 최근에는 서비스형 DDoS 경제의 등장[10, 15, 17]과 함께 DDoS 공격이 더욱 대중화되고 있으며, 1Tbps 이상의 DDoS 공격이 입증되었습니다[2]. 이러한 공격은 일반적으로 피해자에게 막대한 금전적 손실을 가져옵니다. 이에 따라 트래픽 우회를 통해 트래픽을 정화하는 DDoS 방어 서비스(DPS) 시장이 최근 급성장하고 있습니다[9].

트래픽 전환을 사용하면 상시 또는 온디맨드 방식으로 트래픽을 DPS 인프라를 통해 라우팅할 수 있습니다. 트래픽을 우회하는 방법에는 DNS(도메인 이름 시스템) 기반 방법과 BGP(보더 게이트웨이 프로토콜) 기반 방법 등 두 가지 주요 접근 방식이 있습니다. DNS 기반 방식은 적절한 도메인 이름 구성을 통해 네트워크 트래픽을 우회합니다.

M. H. Au 외. (Eds.): NSS 2018, LNCS 11058, 463-473쪽, 2018.
https://doi.org/10.1007/978-3-030-02744-5_34

서버 또는 애니캐스트 기술. 이는 콘텐츠 전송 네트워크(CDN)에서 수행되는 것과 유사합니다. BGP 기반 방식은 고객의 IP 서브넷을 발표하여 스크러빙을 위해 트래픽을 DPS 인프라로 전환합니다. 최근 연구에서 DNS 기반 접근 방식을 측정했지만[9], BGP 기반 DPS의 동작에 대해서는 알려진 바가 거의 없습니다.

이러한 간극을 메우기 위해 이 백서에서는 BGP 메시지의 동역학을 분석하여 BGP 기반 DPS의 동작에 대한 첫 번째 연구를 수행합니다. BGP는 사실상 인터넷의 도메인 간 프로토콜로, 자율 시스템(AS)을 통해 패킷이 라우팅되는 방식을 제어합니다. BGP 역학에 대한 더 나은 이해를 제공하기 위해 Route Viewers Project 및 RIPE와 같은 여러 프로젝트에서 분산된 유리한 지점을 통해 에지 라우터의 업데이트 정보를 계속 수집하고 있습니다. 분석은 두 단계로 구성됩니다. 먼저, 실제 DDoS 이벤트를 특성화할 수 있는 데이터가 부족하기 때문에 머신 러닝 기반 접근 방식을 설계하여 BGP 업데이트 메시지에서 DDoS 이벤트를 식별합니다. 지진, 허리케인, 정전 등 다른 파괴적인 이벤트도 BGP 역학을 교란할 수 있기 때문에 BGP 업데이트 메시지에서 DDoS 이벤트를 식별하는 것은 간단하지 않습니다. 이 문제를 해결하기 위해 먼저 BGP 이상 징후를 탐지한 다음 머신 러닝 기반 방법을 설계하여 BGP 이상 징후가 DDoS 공격으로 인한 것인지 여부를 판단합니다.

분류기를 훈련시키기 위해 비정상적인 BGP 역학을 유발하는 것으로 보고된 충분한 수의 DDoS 공격과 재해 이벤트를 수집합니다. 각 이벤트에 대해 라우트 뷰 프로젝트에서 보고된 기간 동안의 BGP 업데이트 메시지를 수집한 다음, 고정된 시간 간격 내의 BGP 업데이트 메시지에서 특징을 추출합니다. 이벤트를 두 가지 범주로 분류한 후 DDoS 공격과 재해로 분류한 후, 데이터를 사용하여 무작위 포리스트 분류기를 학습시키고, 이 분류기는 다른 탐지된 비정상 이벤트의 유형을 결정하는 데 활용됩니다. 보다 정확하게는 DDoS 공격 이벤트가 식별되면 BGP 트래픽에 대한 심층 분석을 수행하여 BGP 기반 DPS가 공격을 완화하기 위해 BGP를 활용하는 방식을 특성화합니다. 접근 방식을 평가하기 위해 DDoS 공격과 DPS 정책에 대한 후향적 연구를 수행하며 실험 결과를 통해 접근 방식의 효과를 입증합니다. 요약하면 다음과 같습니다:

(1) BGP 업데이트 메시지를 분석하여 DDoS 이벤트를 식별하는 새로운 머신 러닝 기반 접근 방식을 제안합니다.
(2) DDoS 공격이 발생한 후 BGP 기반 DPS의 동작에 대한 첫 번째 분석을 수행

합니다.

(3) 새로운 알고리즘을 기반으로 새로운 시스템을 개발하고 실제 DDoS 공격과 관련된 BGP 데이터를 통해 평 가 합 니 다 .

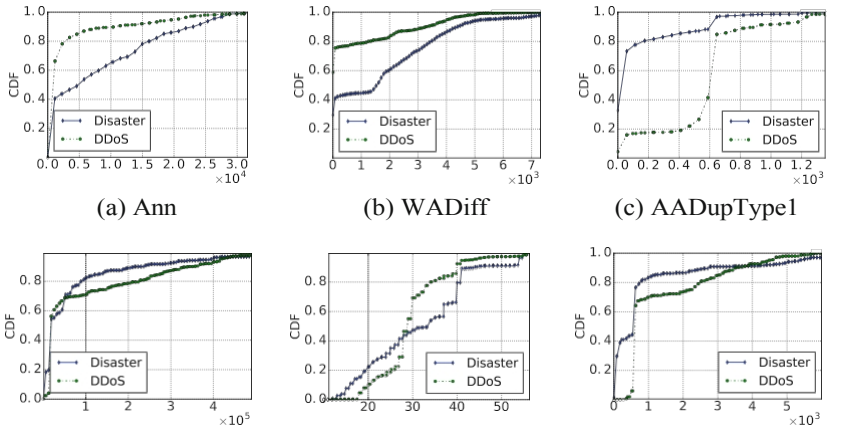
본 논문의 나머지 부분은 다음과 같이 구성됩니다: 2장에서는 추출된 특징의 특성을 분석합니다. 2절에서는 추출된 특징의 특성을 분석합니다. 3장에서는 설계된 시스템에 대해 설명합니다. 4절에서는 시스템의 평가 결과를 설명합니다. 4장에서는 시스템을 검증합니다. 4장에서는 광범위한 실험을 통해 시스템을 검증합니다. 5절에서 관련 문헌을 검토한 후 6절에서 본 연구를 마무리합니다.

2 특징 분석

BGP 업데이트 메시지에서 BGP 트래픽의 변동을 특징짓는 6가지 특징을 조사합니다. 표 1은 특징에 대한 설명을 보여줍니다. 이 특징들은 [12, 19]에서 차용한 것입니다. 그림 1은 다양한 유형의 인시던트에서 특징의 분포를 보여줍니다.

표 1. 기능 설명

특징	정의
Ann	BGP 발표자가 일반화한 발표 건수
WADiff	명시적 철회 후 새로 발표된 경로 수
AADupType1	동일한 IP 접두사에 대한 중복 공지 횟수
Unq pfx_ as	AS가 생성한 고유 접두사 수
최대_ AS_ 경로 len_	AS-PATH의 최대 길이
PFX_ org_ chg	접두사 오리진 변경 횟수



(a) Ann (b) WADiff (c) AADupType1

(d) Unq pfx_ as 기능 (e) 최대_ AS_ 경로 len_ (f) Asn_ prfx_ chg

그림 1. 기능의 CDF

Ann은 탐지 주기에서 BGP 스피커가 발표하는 경로의 수입니다. 그림 1(a)는 Ann 기능이 DDoS 이벤트와 재해 이벤트를 구분하는 데 도움이 될 수 있음을 보여줍니다. DDoS 이벤트는 발표 횟수 값이 3000 미만인 비정상 데이터빈

이 약 80%에 달하는 것으로 나타났습니다. 그러나 재해 이벤트에서는 3000 미만의 값을 가진 비정상 데이터빈이 50%를 넘지 않습니다. 이는 DDoS 공격에서 전송되는 알림 수가 재해 이벤트에서 전송되는 알림 수보다 적다는 것을 나타냅니다. 그 이유는 재해 이벤트는 일반적으로 오랫동안 지속되므로 경로를 사용할 수 없게 되면 엣지 라우터가 새로운 경로를 발표하기 때문일 수 있습니다.

WADiff는 명시적 철회 후 새로 발표된 경로의 수입니다. 이전에 발표된 경로가 철회되면 철회된 경로에 의존하는 다른 경로가 계속 선택되어 발표되다가 하나씩 제거될 수 있으며[3], 이로 인해 인터넷의 수렴이 느려지게 됩니다. 탈퇴 메시지의 전송 여부에 따라 명시적 탈퇴와 묵시적 탈퇴를 구분합니다. 명시적 철수는 철수 메시지와 관련된 철수이며, 암시적 철수는 철수 메시지 없이 기존 경로가 목적지 접두사에 대한 새로운 경로의 발표로 대체되는 경우 발생합니다. 그림 1(b)는 재난 발생 시 명시적 철수 후 새로 발표된 경로가 더 많다는 것을 보여줍니다. 이는 재해 이벤트가 발생하면 일반적으로 일부 BGP 경로에 연결할 수 없게 되어 피어 라우터가 명시적 철회를 전송하기 때문입니다.

AADupType1은 모든 필드가 변경되지 않은 상태에서 동일한 접두사에 대한 중복 발표 횟수입니다. Park 등[16]은 BGP 트래픽에서 중복 알림의 원인을 연구한 결과, eBGP와 iBGP 간의 의도하지 않은 상호작용으로 인해 중복이 발생한다는 사실을 발견했습니다. 라우터는 iBGP 속성 값만 다른 iBGP를 통해 업데이트를 수신하므로 라우터는 업데이트가 고유한 것으로 간주합니다. 그러나 라우터가 업데이트를 처리하고 iBGP 속성 값을 제거한 후 해당 업데이트를 eBGP 피어로 전송하면 두 업데이트는 eBGP 피어의 관점에서 동일하게 보입니다[16]. 따라서 AS의 변경 경로가 많을수록 중복 알림이 많아집니다. 그림 1(c)는 이 특징의 분포를 보여줍니다. DDoS 공격의 분포는 500개에서 600개로 급격히 증가하는 것을 볼 수 있습니다. 이는 DDoS 공격이 일반적으로 피해자의 유사한 대응(예: 영향을 받은 경로를 반복적으로 알리는 것)으로 이어진다는 것을 나타냅니다.

주어진 기간 동안 AS에서 발생한 고유 접두사 수를 의미합니다. 이웃 피어들이 주고받은 공지 및 인출 횟수는 불안정한 기간 동안 중요한 특징입니다. 저희는 이 특징을 활용해 정상 상태의 안정적인 상황을 모델링합니다. 그림 1(d)를 보면 이 기능이 DDoS 이벤트 기간보다 재난 이벤트 기간에 더 안정적이라는 것을 알 수 있습니다. 그 이유는 DDoS 공격이 발생하면 DPS 사업자는 피해자가 속한 접두사를 발표하여 DDoS 공격 트래픽을 완화하는 BGP 기반 방식을 활용하기 때문에 고유 접두사의 수가 증가하기 때문입니다.

최대-AS-경로-길이란 특정 기간 동안 BGP 라우터가 발표하는 AS 경로의 최대 길이입니다. 정상적인 상태에서는 BGP 프로토콜이 짧은 경로를 선호하기

때문에 BGP 라우터가 발표하는 AS 경로는 일반적으로 홉 수가 제한되어 있습니다. 그러나 AS가 공격을 받는 경우 운영자는 AS 경로 필드에 중복된 여러 개의 AS를 사전 보류하여 암묵적으로 사전 발표된 경로를 철회할 수 있습니다. 이렇게 하면 AS 경로의 길이가 크게 늘어날 수 있습니다. 그림 1(e)는 DDoS 공격 이벤트의 AS 경로 길이가 25~30개 범위에 집중되어 있어 분포 곡선이 급격하게 증가하는 것을 보여줍니다. 그러나 재해 이벤트의 최대 AS 경로 길이 분포는 DDoS 공격의 경우보다 훨씬 더 고르게 분포되어 있습니다. 이는 재해 이벤트는 일반적으로 인터넷 중단을 유발하기 때문에 재해 이벤트가 발생하는 동안 더 긴 경로가 존재하기 때문입니다.

ASN(AS 번호)은 AS를 식별하는 데 사용되는 전 세계적으로 고유한 번호입니다. 이를 통해 AS는 인접한 AS 간에 외부 라우팅 정보를 교환할 수 있습니다. Asn prfx chg는 일정 기간 동안 AS의 접두사 변경 횟수입니다. 이 기능은 인터넷 토폴로지가 자주 변경되지 않아야 한다는 가정 하에 제안되었습니다. 이 기능은 접두사 하이재킹 공격을 탐지하기 위한 단일 BGP 기능으로 사용되었습니다. 그러나 AS가 DPS AS를 통해 서브넷의 트래픽을 리라우팅하기 위해 접두사를 변경하는 것도 가능합니다. 그림 1(f)는 DDoS 공격 중에 접두사 오리진 변경이 더 많이 발생한다는 것을 보여줍니다. 그 이유는 DDoS 공격 이벤트가 발생하면 DPS 제공업체가 피해자의 접두사를 발표하고 트래픽을 스크러빙하기 때문입니다.

3 시스템 설계

그림 2는 조사 프로세스의 개요를 보여줍니다. 이 프로세스는 훈련 단계와 모니터링 단계로 구성됩니다. 두 단계 모두에서 고정된 시간 간격 내에 BGP 업데이트 데이터에서 여러 가지 특징을 추출합니다. 이 백서의 나머지 부분에서는 추출된 특징을 벡터로 그룹화하여 데이터빈이라고 합니다. DDoS 공격이 식별되면 방어 정책 분석 모듈을 통해 DPS의 AS에서 발생한 BGP 업데이트 트래픽을 추가로 분석합니다. 우리는 64비트 Windows 10 시스템(Intel(R) CUP Q9550 @2.83GH 및 8.0GB RAM)에서 실행되는 Python을 사용하여 시스템의 프로토타입을 개발합니다.

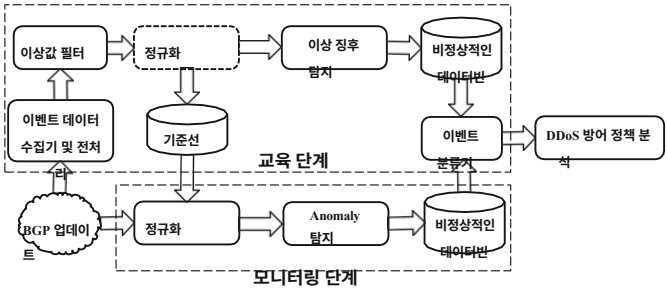


그림 2. 시스템 아키텍처

3.1 교육 단계

먼저 허리케인, 정전, 지진, 케이블 절단, DDoS 공격 등 BGP 변경을 유발할 수 있는 다양한 종류의 이벤트 를 수집합니다. 이러한 이벤트에 대한 관련 뉴스를 직접 검색하여 이벤트의 발생 시간을 파악합니다. 훈련 단계에서는 이러한 이벤트가 발생한 시간대의 BGP 업데이트 데이터를 수집합니다. BGP 트래픽은 본질적으로 동적이며 정상 상태에서도 일부 이상값이 존재하기 때문에, 정상 기간의 이상값 데이터 빈을 걸러내기 위해 k-평균 방법을 사용합니다[12]. 구체적으로, 정상 기간의 데이터 빈은 다음과 같이 클러스터링됩니다.

을 유클리드 거리에 따라 두 그룹으로 나눕니다. 대다수 그룹은 정상 데이터빈만 포함할 것으로 예상되며 정상성의 기준선으로 사용됩니다. 발생 기간에 정상 데이터빈이 다수 포함되도록 하기 위해 정상 데이터빈과 발생 기간의 데이터빈을 혼합합니다. 여기서도 *k-평균* 방법을 사용하여 혼합된 데이터빈을 두 그룹으로 클러스터링합니다. 다수의 데이터빈 중 하나는 정상 데이터빈으로, 다른 하나는 비정상 데이터빈으로 구분합니다. 이렇게 얻은 비정상 데이터빈을 타임스탬프에 따라 다시 그룹화하여 연속적인 비정상 데이터빈을 얻습니다. 이러한 연속 비정상 데이터빈은 두 가지 요건을 충족합니다: (1) 그 간격이 3분 미만이고 (2) 클러스터에 연속된 데이터빈이 3개 이상이 어야 합니다. 이렇게 얻은 연속적인 비정상 데이터빈 그룹을 '인시던트'라고 합니다.

둘째, 인시던트의 유형에 수동으로 레이블을 지정합니다. 이 백서에서는 재해 이벤트와 DDoS 공격만 구분합니다. 41개의 과거 이벤트를 수집하고 인시던트의 유형에 수동으로 라벨을 붙였습니다. 결과는 표 2에 요약되어 있으며 이러한 이벤트를 사용하여 랜덤 포레스트 방법의 분류 모델을 훈련합니다. 재해 이벤트와 DDoS 공격 이벤트만 구분합니다. 시스템의 정확도를 평가하기 위해 5배 교차 검증 방법을 사용합니다. 각 카테고리에서 탐지된 이상 데이터 빈을 5배수로 나누고, 각 테스트에서 5배수 중 하나는 테스트 데이터로, 나머지 4배수는 학습 데이터로 사용합니다. 결과는 5개의 결과를 평균하여 얻습니다. 수집된 데이터를 기반으로 91.2%의 정확도를 얻었습니다.

표 2. 데이터 세트 요약

유형	이벤트 번호	감지된 데이터빈
허리케인	4	30
블랙아웃	4	14
지진	4	152
케이블 컷	9	602
DDoS	20	889

3.2 모니터링 단계

모니터링 단계에서는 학습 단계에서 얻은 기준선을 사용하여 새로 수집된

BGP 업데이트 메시지를 노멀라이즈합니다. 더 정확히 말하면, 이 백서에서는 데이터빈을 정규화하기 위해 Z-score 정규화 방법을 사용합니다. 특징의 Z점수 값은 $z = \frac{x-\mu}{\sigma}$ 로 계산되며, 여기서 μ는 *구한* 정규 데이터빈의 평균이고 σ는 표준 편차입니다. 계산된 평균과 편차는 모니터링 단계에서 데이터빈을 정규화하는 데 사용됩니다. 이상 징후 감지 모듈은 BGP 역학에 이상 징후가 있는지 여부를 감지합니다. 이상 징후가 감지되면 시스템은 학습된 분류기를 활용하여 비정상 이벤트가 DDoS 공격으로 인한 것인지 여부를 식별합니다.

이 시스템을 통해 실무자가 자신의 경험 지식을 활용하여 시스템의 성능을 개선할 수 있다는 점은 주목할 가치가 있습니다. 알람 발생 시

이 제기되면 실무자는 다른 외부 정보 소스를 기반으로 결과에 대한 판단을 내릴 수 있습니다. 예측이 실무자의 판단과 일치하면 새로 들어오는 데이터빈이 학습 데이터빈에 추가됩니다. 그렇지 않으면 예측이 거부됩니다.

3.3 완화 정책 분석

DPS에서 사용하는 BGP 기반 방어 정책을 분석하는 모듈을 제공합니다. DDoS 이벤트가 확인된 후 이 모듈을 사용하여 DPS에서 채택한 BGP 정책을 검토합니다. 실무자가 자신의 경험과 지식을 활용하여 시스템 성능을 개선할 수 있다는 점도 주목할 만합니다. 경보가 발생하면 실무자는 다른 외부 정보 소스를 기반으로 결과에 대한 판단을 내릴 수 있습니다. 예측이 실무자의 판단과 일치하면 새로 들어오는 데이터빈이 학습 데이터빈에 추가됩니다. 그렇지 않으면 예측이 거부됩니다.

DPS 제공업체가 채택한 정책을 자동으로 추출하는 알고리즘을 개발했습니다. DPS 제 공 업 체 는 고객이 DDoS 공격을 받고 있는 것을 발견하면 BGP 프리엔딩을 수행할 수 있습니다. 프리엔딩은 AS 경로의 왼쪽에 하나 이상의 AS 번호를 추가하는 것을 의미합니다. 일반적으로 이 작업은 자신의 AS 번호를 사용하여 수행되며, 다른 사람의 AS 번호를 사용하면 의도하지 않은 부작용이 발생할 수 있습니다. 이러한 보호 프로세스는 WADiff BGP 업데이트 메시지로 시작하여 AW BGP 업데이트 메시지로 끝납니다. 이 프로세스를 B_0 로 표시합니다. 선행 조치에서 ASN은 BGP 라우팅 경로에 나타나고 WADup BGP 업데이트 메시지는 AW BGP 업데이트 메시지 다음에 나옵니다. 직접 보호 동작은 DPS 제공업체의 ASN이 BGP 라우팅 경로의 첫 번째 홉 역할을 하는 동작으로 정의하며, AADiff BGP 업데이트 메시지는 AADiff BGP 업데이트 메시지 뒤에 따라오게 됩니다. 선행 액션을 B_1 로, 지시된 보호 액션을 B_2 로 표시합니다. 알고리즘은 다음과 같이 작동합니다. 먼저, 각 피해자 접두사에 대해 AW, WWDup, AADupType1, AADupType2, AADiff, WADup, WADiff 태그로 BGP 업데이트 레코드에 레이블을 지정합니다. BGP 업데이트 메시지에 레이블을 지정한 후, 피해자를 보호하기 위해 DPS 제공업체가 채택한 정책을 반영하는 B_0 , B_1 및 B_2 시퀀스를 인식합니다.

4 실험

4.1 DDoS 공격 탐지 평가

저희 시스템은 2016년 10월에 Dyn에 대한 DDoS 공격을 탐지하는 데 성공했습니다[8]. 2016년 10월 21일, Dyn은 관리되는 DNS 네트워크의 성능을 소모하는 대규모 클라이언트의 DNS 쿼리로 인해 어려움을 겪었습니다. 이로 인해 Dyn의 DNS 서비스를 사용할 수 없게 되었습니다. 이로 인해 수많은 웹사이트 연결에 어려움을 겪게 됩니다. 공격이 진행되는 동안 다른 DNS 공급업체로 이동하는 트래픽이 급격히 증가하여 네트워크 트래픽이 광범위하게 혼잡해졌습니다. 이러한 혼잡은 결국 BGP 트래픽의 비정상적인 동적 변화를 초래하여 BGP 동적 변화를 통해 Dyn DDoS 공격 이벤트를 감지할 수 있게 되었습니다.

그림 3은 시간 대비 영향력 값을 보여줍니다. 정규화된 특징과 기준선 사이의 차이의 합인 영향값은 데이터빈과 정상 데이터빈의 거리를 나타냅니다. 2016년 10월 21일의 세 가지 비정상적인 역학 관계는 세 개의 빨간색 블록으로 표시되어 있습니다. 저희의 이상 징후 탐지 모듈은 이러한 비정상적인 데이터빈을 식별하여 DDoS 공격으로 정확하게 분류할 수 있습니다. 탐지된 이상 기간은 다음과 같습니다:

- 첫 번째 기간은 04:30:22(PDT)에 시작되었고 BGP 트래픽의 변동이 시작되었습니다. 06:16:00(PDT) 경까지 변동이 줄어들었습니다. 이는 보고된 사고의 시작 및 완화 시간과 일치합니다[18]. 이 기간 동안 아시아 태평양과 동유럽에 있는 Dyn의 DNS 서버 플랫폼에 대규모 요청이 발생한 후 미국 동부 지역에서도 대규모 요청이 발생하여 BGP 경로 변동이 발생했습니다[8].
- 시스템 탐지 결과에 따르면 두 번째 기간은 08:41:44(PDT)에 시작하여 10:32:00(PDT) 경에 종료되었으며, 이는 보고된 DDoS 공격 기간과 일치합니다[1].
- 저희 시스템은 또한 13:19:28에 시작하여 14:08:0(PDT) 경에 종료된 세 번째 비정상적인 BGP 역학 패턴을 감지했습니다. 이는 뉴스에 보도된 디도스 공격 기간과도 일치합니다[8].

또한 그림 3에서 녹색 블록으로 표시된 것처럼 각각 01:22:23(PDT)과 17:47:1에 시작된 BGP 트래픽에서 몇 가지 명백한 변동이 추가로 발견되었습니다. 그러나 이러한 이벤트는 Dyn.com이나 다른 뉴스 미디어에서 보고되지 않았습니다. 이러한 이벤트는 DDoS 공격의 시작과 여진으로 인해 발생한 것으로 추정됩니다(표 3).

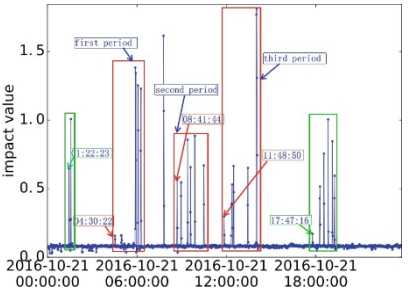


그림 3. Dyn DDoS 공격 개요

5 관련 작업

많은 연구에서 BGP 동역학의 불안정성 또는 병리적 동작을 탐지하는 방법을 에서 다루었습니다. Labovitz 등[11]은 BGP 라우팅 메시지를 조사한 결과 라우팅 업데이트의 양이 예상보다 많다는 사실을 발견했습니다.

표 3. 접두사 3개로 구성된 업데이트 패턴 시퀀스의 DPS 보호 동작

접두사	패턴 시퀀스 업데이트
58.64.128.119/32	WADiff→B1→B1→B1→B2→B1→AW
58.64.138.186/32	WADiff→B1→B1→B2→AW
58.64.135.102/32	B0→B0

또한, 이들은 포워딩 불안정성과 라우팅 정책 변동에 대한 몇 가지 예상치 못한 추세를 밝혀냈습니다. Deshpande 등[6]은 통계적 패턴 인식 기법을 적용하여 GBP 역학의 불안정성을 감지하는 온라인 불안정성 감지 아키텍처를 제안했습니다. 이들은 AS 경로 길이와 AS 경로 편집 거리와 같은 특징이 인터넷 토폴로지의 동작을 모델링하는 데 매우 효과적이라는 것을 발견했습니다. Chang 등[4]은 BGP 업데이트 스트림에서 도메인 간 경로 변경 이벤트를 식별하는 알고리즘을 제안했습니다. Feldmann 등[7]은 BGP 업데이트에서 라우팅 불안정성의 원인을 식별하는 방법론을 제안했습니다. 여러 연구에서 통계적 패턴 인식 기법을 활용하여 BGP 라우팅 동역학의 불안정성을 탐지했습니다[6, 11, 13]. 이러한 연구와 비교하여 본 논문에서는 비정상적인 BGP 동역학의 두 가지 주요 원인인 DDoS 공격 이벤트와 중단성 재해 이벤트를 구분하는 머신 러닝 기반 방법을 제안합니다. 이를 통해 BGP 트래픽 이상 징후가 감지될 때 DDoS 공격이 진행 중인지 여부를 식별할 수 있습니다.

정전, 케이블 절단, 웜, 접두사 하이재킹 공격 등과 같은 역사적 사건으로 인한 영향을 분석하여 많은 후향적 연구도 수행되었습니다. Cowie 등[5]은 2001년 7월과 9월에 각각 발생한 코드 레드 II와 님다 웜으로 인한 글로벌 BGP 라우팅 불안정성을 분석했습니다. 그 결과 블랙아웃 지역에서 그 영향이 공개된 것보다 더 심각하다는 것을 발견했습니다. Li 등[14]은 대규모 정전 시 BGP의 행동을 글로벌 및 접두사 수준의 관점에서 분석했습니다. 그 결과 글로벌 수준에서 인출 건수가 증가한다는 사실을 발견했습니다. 결과적으로 접두사 수준에서는 에지와 노드 수가 급격히 감소했습니다. 이러한 연구는 주로 중단 이벤트가 BGP 라우팅 성능에 미치는 영향에 관한 것입니다. 이 백서에서는 DDoS 공격으로 인한 중단과 다양한 DPS 정책의 영향에 중점을 둡니다.

6 결론

이 백서에서는 BGP 기반 DDoS 방어 서비스의 동작을 조사합니다. 지진, 정전, 케이블 절단 등과 같은 다른 장애 이벤트가 아닌 DDoS 공격으로 인한 비정상적인 BGP 다이내믹스를 식별하기 위해 BGP 다이내믹스의 비정상적인 행동을 유발하는 것으로 입증된 40개 이상의 수동 분류 이벤트 데이터셋을 기반으로 적절한 분류기를 학습시킵니다. 또한 비정상적인 BGP 업데이트 메시지를 통해 DDoS 이벤트를 탐지하는 시스템을 개발하고 일반적인 DDoS 공격에 대한 DPS의 동작을 분석하는 새로운 알고리즘을 설계합니다. 이 시스템을 실제

DDoS 공격에 대해 DPS가 공격을 완화하는 데 사용하는 정책을 파악하고 몇 가지 의미 있는 결과를 얻었습니다. 이 연구는 효과적인 DDoS 공격 방어 체계의 설계에 대해 조명합니다.

감사의 말. 이 논문에서 제시된 연구는 국립자연과학재단(번호 61602370, 61672026, 61772411, U1736205), 박사 후 재단(번호 201659M2806, 2018T111066), 중앙대학 기초연구기금(번호. 1191320006), 산시 박사후 재단, 프로젝트 JCYJ20170816100819428 지원, CCF-텐센트 오픈 펀드 위뱅크 특별 기금(CCF-Webank RAGR20180101), CCF-NSFOCUS Kun- Peng 연구 기금(CCF-NSFOCUS 2018006호).

참조

1. 금요일 미국에 대한 대규모 디도스 공격이 어떻게 일어났는지 https://en.wikipedia.org/ wiki/2016 Dyn 사이버 공격 인용 노트 - 유선 - 5/
2. OVH, 1.1Tbps DDoS 공격을 받다. https://www.scmagazineuk.com/ovh- suffers-11tbps-ddos-attack/article/532197/. 2017년 3월 11일 액세스 됨
3. 찬드라셰카르, J., 두안, Z., 장, Z.L., 크라스키, J.: BGP에서 경로 탐색 제한. In: 제24회 INFOCOM 연례 공동 컨퍼런스, 4권, 2337-2348쪽. IEEE (2005)
4. Chang, D.F., Govindan, R., Heidemann, J.: BGP 경로 변경의 시간적 및 위상학적 특성. In: ICNP, 190-199쪽. IEEE (2003)
5. Cowie, J., Ogielski, A.T., Premore, B., Yuan, Y.: 인터넷 웜과 글로벌 라우팅 불안정성. In: ITCom 2002: 정보 기술과 통신의 융합, 195-199쪽 (2002)
6. Deshpande, S., Thottan, M., Ho, T.K., Sikdar, B.: BGP 불안정성 감지 및 분석을 위한 온라인 메커니즘. IEEE Trans. Comput. **58**(11), 1470-1484 (2009)
7. 펠드만, A., 매넬, O., 마오, Z.M., 버거, A., 매그스, B.: 인터넷 라우팅 불안정성 찾기. ACM SIGCOMM CR **34**, 205-218 (2004)
8. Hilton, S.: 10월 21일 금요일 공격에 대한 Dyn 분석 요약. http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
9. Jonker, M., Sperotto, A., van Rijswijk-Deij, R., Sadre, R., Pras, A.: DDoS 방어 서비스 도입 측정. In: 2016 ACM 인터넷 측정 컨퍼런스 논문집, 279-285쪽. ACM (2016)
10. 카라미, M., 맥코이, D.: 서비스형 DDoS의 새로운 위협에 대한 이해. In: LEET (2013)

11. Labovitz, C., Malan, G.R., Jahanian, F.: 인터넷 라우팅 불안정성. IEEE/ACM Trans. **6**(5), 515-528 (1998)
12. 리, J., 브룩스, S.: I-지진계: 인터넷 지진 관측 및 측정. In: INFOCOM, 2011 Proceedings IEEE, 2624-2632쪽. IEEE (2011)
13. Li, J., Guidero, M., Wu, Z., Purpus, E., Ehrenkranz, T.: BGP 라우팅 동역학 재검토. ACM SIGCOMM CR **37**(2), 5-16 (2007)
14. Li, J., Wu, Z., Purpus, E.: Cam04-5: 대규모 정전 시 BGP의 동작을 이해하기 위해. In: IEEE Globecom. IEEE (2006)
15. Noroozian, A., Korczyn´ski, M., Gan˜an, C.H., Makita, D., Yoshioka, K., van Eeten, M.: 누가 부팅을 받는가? 서비스형 DDoS에 의한 피해 분석. In: Monrose, F., Dacier, M., Blanc, G., Garcia-Alfaro, J. (eds.) RAID 2016. LNCS, vol. 9854, 368-389 쪽. 스프링거, 참 (2016). https://doi.org/10.1007/978-3-319-45719-2 17

16. Park, J.H., Jen, D., Lad, M., Amante, S., McPherson, D., Zhang, L.: BGP 공지사항의 중복 업데이트 발생 조사. In: Krishnamurthy, A., Plattner, B. (eds.) PAM 2010. LNCS, vol. 6032, 11-20쪽. 스프링거, 하이델베르크 (2010). https://doi.org/10.1007/978-3-642-12334-4 2
17. Santanna, J.J., et al: 부터-서비스형 DDoS 공격에 대한 분석. In: 2015 통합 네트워크 관리(IM)에 관한 2015 IFIP/IEEE 국제 심포지엄, pp. 243-251. IEEE (2015)
18. 스미스, D.: 금요일의 미국 대규모 디도스 공격 발생 경위 https://blog.radware.com/security/2016/10/fridays-massive-ddos-attack-u-s-happened/.
19. Zhang, M.: BGPInspector: 실시간 확장 가능한 국경 게이트웨이 프로토콜 모니터링 프레임워크. CAS (2014)