Understanding the Behaviors of BGP-based DDoS Protection Services

Tony Miu Tung1, Chenxu Wang2,3(B) , and Jinhe Wang2

1 Nexusguard Ltd., Tsuen Wan, 홍콩

2 School of Software Engineering, 시안 교통대학교, 시안, 중국 cxwang@mail.xjtu.edu.cn

3 MoE Key Laboratory for INNS, 시안 교통대학교, 시안 710049, 중국

1 Introduction

DDoS(분산 서비스 거부) 공격은 수십 년 동안 인터넷 인프라를 위협해 왔습니다. 최근 몇 년 동안 DDoS-as-a-Service 경제의 출현으로 DDoS 공격이 더욱 대중화되고 있으며[10,15,17] 1Tbps 이상의 DDoS 공격이 입증되었습니다[2]. 이러한 공격은 일반적으로 피해자에게 막대한 재정적 손실을 초래합니다. 그 결과, 트래픽 전환을 통해 트래픽을 정화하는 DDoS 방어 서비스(DPS) 시장은 최근 급격히 성장하고 있습니다[9]. 트래픽 전환을 사용하면 DPS 인프라를 통해 상시 또는 온디맨드 방식으로 트래픽을 라우팅할 수 있습니다. 트래픽을 전환하는 방법에는 DNS(Domain Name System) 기반 방법과 BGP(Border Gateway Protocol) 기반 방법 등 두 가지 주요 방법이 있습니다. DNS 기반 접근 방식은 도메인 이름 서버 또는 애니캐스트 기술의 적절한 구성을 통해 네트워크 트래픽을 전환합니다. 콘텐츠 전송 네트워크(CDN)에서 수행되는 작업과 유사합니다. BGP 기반 체계는 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.

이 격차를 해소하기 위해 이 백서에서는 BGP 메시지의 역학을 분석하여 BGP 기반 DPS의 동작에 대한 첫 번째 연구를 수행합니다. BGP는 인터넷의 사실상의 도메인 간 프로토콜이며 패킷이 AS(Autonomous System)를 통해 라우팅되는 방식을 제어합니다. BGP 역학을 더 잘 이해하기 위해 Route Viewers Project 및 RIPE와 같은 여러 프로젝트는 분산된 유리한 지점을 통해 에지 라우터의 업데이트 정보를 계속 수집합니다. 분석은 두 단계로 구성됩니다. 첫째, 실제 DDoS 이벤트를 특성화하기 위한 데이터가 일반적으로 부족하기 때문에 BGP 업데이트 메시지에서 DDoS 이벤트를 식별하기 위한 기계 학습 기반 접근 방식을 설계합니다. 지진, 허리케인, 정전과 같은 다른 파괴적인 이벤트도 BGP 역학을 방해할 수 있기 때문에 BGP 업데이트 메시지에서 DDoS 이벤트를 식별하는 것은 간단하지 않습니다. 이 문제를 해결하기 위해 먼저 BGP 이상을 감지한 다음 BGP 이상이 DDoS 공격으로 인한 것인지 여부를 확인하는 기계 학습 기반 방법을 설계합니다.

분류자를 훈련시키기 위해 비정상적인 BGP 역학을 유발하는 것으로 보고된 충분한 수의 DDoS 공격 및 재해 이벤트를 수집합니다. 각 이벤트에 대해 경로 보기 프로젝트에서 보고된 기간 동안 BGP 업데이트 메시지를 수집한 다음 고정된 시간 간격 내에 BGP 업데이트 메시지에서 기능을 추출합니다. 이벤트를 DDoS 공격과 재해의 두 가지 범주로 분류한 후 데이터를 사용하여 랜덤 포레스트 분류기를 훈련하고 이를 사용하여 감지된 다른 비정상 이벤트의 유형을 결정합니다. 보

다 정확하게는 DDoS 공격 이벤트가 식별되면 BGP 트래픽에 대한 심층 분석을 수행하여 BGP 기반 DPS가 BGP를 활용하여 공격을 완화하는 방법을 특성화합니다. 접근 방식을 평가하기 위해 DDoS 공격 및 DPS 정책에 대한 후향적 연구를 수행하며, 실험 결과는 접근 방식의 효과를 입증합니다. 요약하면, 우리는 다음과 같은 기여를 합니다.

(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 수행합니다.

(3) 새로운 알고리즘을 기반으로 새로운 시스템을 개발하고 실제 DDoS 공격과 관련된 BGP 데이터를 통해 평가합니다.

이 논문의 나머지 부분은 다음과 같이 구성되어 있습니다. 섹션 2에서는 추출된 특징의 특성을 분석합니다. 섹션 3에서는 설계된 시스템에 대해 설명합니다. 섹션 4에서는 시스템의 평가 결과에 대해 설명합니다. 섹션 4에서는 광범위한 실험을 통해 시스템을 검증합니다. 섹션 5의 관련 문헌을 검토한 후, 섹션 6에서 이 작업을 마칩니다.

2 Feature Analysis

BGP 트래픽의 변동을 특성화하기 위해 BGP 업데이트 메시지의 6가지 기능을 조사합니다. 표 1 에는 기능에 대한 설명이 표시되어 있습니다. 이러한 기능은 [12,19]에서 차용한 것입니다. 그림 1은 다양한 유형의 인시던트에서 기능의 분포를 보여 줍니다.

표 1. 기능 설명

Features	Definition
Ann	Number of announcements generalized by BGP speakers
WADiff	Number of new announced paths after an explicit withdrawal
AADupType1	Number of duplicate announcements to the same IP prefix
Unq_pfx_as	Number of unique prefixes originated by an AS
Max_AS_path_len	The maximum length of AS-PATHs
pfx_org_chg	Number of Prefix origin change

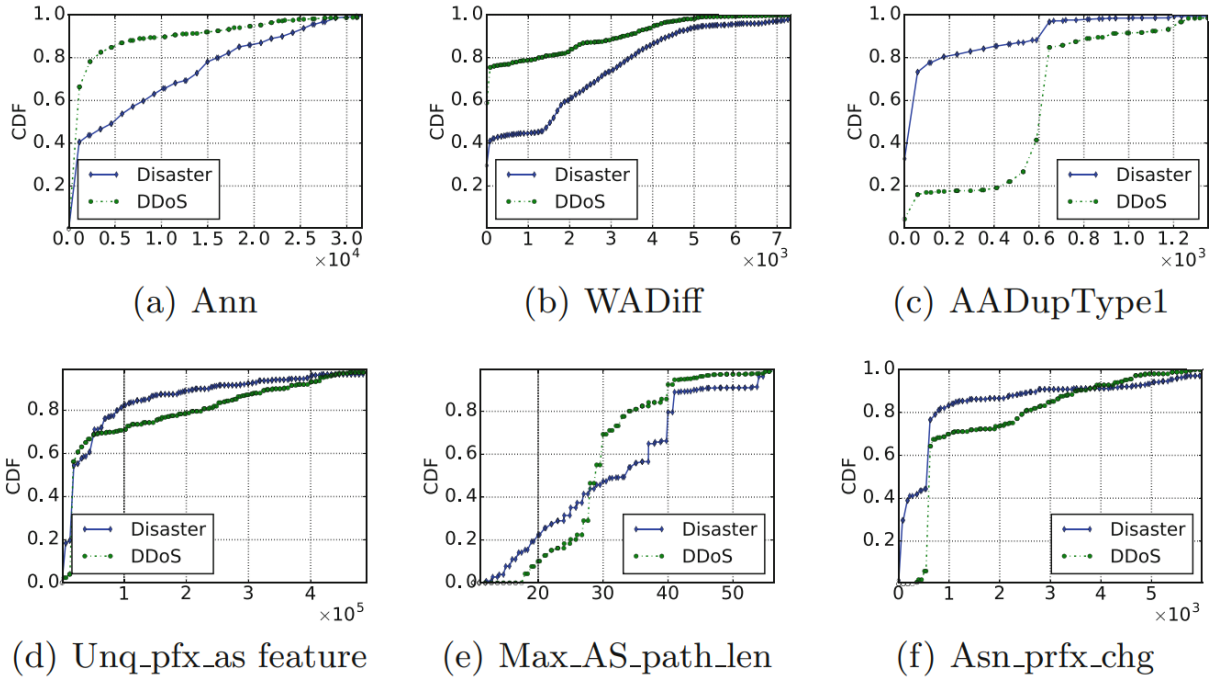

Fig. 1. CDF of the features

Ann은 탐지 주기에서 BGP 스피커가 발표한 경로 수입니다. 그림 1(a)는 Ann 기능이 DDoS 이벤트와 재해 이벤트를 구분하는 데 도움이 될 수 있음을 보여줍니다. DDoS 이벤트에는 공지 횟수 값이 3000개 미만인 비정상 데이터 빈이 약 80%인 것으로 나타났습니다. 그러나 값이 3000 미만인 재해 이벤트에서 검색된 비정상 데이터 빈의 50% 이하입니다. 이는 DDoS 공격에서 전송되는 공지 사항이 재난 발생 시보다 적다는 것을 나타냅니다. 그 이유는 재해 이벤트가 일반적으로 오랫동안 지속되므로 경로를 사용할 수 없으면 에지 라우터가 새 경로를 알리기 때문일 수 있습니다.

WADiff는 명시적 철회 후 새로 발표된 경로의 수입니다. 이전에 발표된 경로가 철회될 때 철회된 경로에 의존하는 다른 경로가 여전히 선택되고 발표될 수 있지만 하나씩 제거될 수 있으며 [3], 이로 인해 인터넷의 수렴이 느려집니다. 우리는 출금 메시지가 전송되었는지 여부에 따라 명시적 또는 묵시적 출금을 구분합니다. 명시적 인출은 인출 메시지와 관련된 인출입니다. 반면 암시적 철회는 기존 경로가 중간 철회 메시지 없이 대상 접두사에 대한 새 경로 발표로 대체될 때 발생합니다. 그림 1(b)는 재난 발생 시 명시적으로 철수한 후 새로 발표된 경로가 더 많다는 것을 보여줍니다. 이는 재해 이벤트로 인해 일반적으로 일부 BGP 경로에 연결할 수 없게 되어 피어 라우터가 명시적 인출을 전송하도록 트리거하기 때문입니다.

AADupType1은 모든 필드가 변경되지 않은 동일한 접두사에 대한 중복 알림 수입니다. Park et al. [16]은 BGP 트래픽에서 중복 알림의 원인을 연구한 결과, eBGP와 iBGP 간의 의도하지 않은 상호 작용으로 인해 중복이 발생한다는 사실을 발견했습니다. 라우터는 iBGP 특성 값만 다른 iBGP를 통해 업데이트를 수신하므로 라우터는 업데이트가 고유하다고 생각합니다. 그러나 라우터가 업데이트를 처리하고, iBGP 특성 값을 제거하고, 업데이트를 eBGP 피어로 전송하면 eBGP 피어

[16]의 관점에서 두 업데이트가 동일하게 보입니다. 따라서 AS에 대체 경로가 많을수록 중복 알림이 많아집니다. 그림 1(c)는 이 특징의 분포를 보여줍니다. DDoS 공격의 분포는 500건에서 600건으로 급격히 증가했습니다. 이는 DDoS 공격이 일반적으로 피해자의 유사한 반응(예: 영향을 받는 경로를 반복적으로 발표)으로 이어진다는 것을 나타냅니다.

Unq pfx as는 지정된 시간 창에서 AS에서 시작된 고유한 접두사의 수입니다. 인접 동종 업체가 교환하는 발표 및 인출 횟수는 불안정 기간 동안 중요한 기능입니다. 이 기능을 활용하여 정상 상태의 안정적인 상황을 모델링합니다. 그림 1(d)에서 이 기능이 DDoS 이벤트 기간보다 재난 이벤트 기간 동안 더 안정적임을 알 수 있습니다. 그 이유는 DDoS 공격이 발생할 때 DPS 공급자가 DDoS 공격 트래픽을 완화하기 위해 피해자에게 속한 접두사를 발표하여 BGP 기반 접근 방식을 잘 활용할 수 있기 때문이며, 이로 인해 고유한 접두사 수가 증가할 수 있습니다.

최대 AS 경로 len 은 특정 시간 창에서 BGP 라우터가 발표한 AS 경로의 최대 길이입니다. 정상적인 상태에서 BGP 라우터가 발표한 AS 경로는 BGP 프로토콜이 짧은 경로를 선호하기 때문에 일반적으로 홉 수가 제한됩니다. 그러나 AS가 공격을 받는 경우, 운영자는 AS-path 필드에 여러 개의 중복된 AS를 미리 삽입하여 사전 발표된 경로를 암시적으로 철회할 수 있습니다. 이로 인해 AS 경로의 길이가 크게 늘어날 수 있습니다. 그림 1(e)는 DDoS 공격 이벤트에 대한 AS 경로의 길이가 25에서 30 사이의 범위에 집중되어 있어 분포 곡선이 급격히 증가했음을 보여줍니다. 그러나 재해 이벤트에 대한 최대 AS 경로 길이의 분포는 DDoS 공격의 경우보다 훨씬 균등합니다. 이는 재해 사건으로 인해 일반적으로 인터넷 중단이 발생하므로 재해 발생 시 경로가 더 길어지기 때문입니다.

ASN(AS 번호)은 AS를 식별하는 데 사용되는 전역적으로 고유한 번호입니다. 이를 통해 AS는 인접 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 가정을 기반으로 제안됩니다. 접두사 하이재킹 공격을 탐지하기 위해 단일 BGP 기능으로 사용되었습니다. 그러나 AS가 DPS AS를 통해 서브넷의 트래픽을 다시 라우팅하기 위해 접두사를 변경할 수도 있습니다. 그림 1(f)는 DDoS 공격 중에 접두사 출처가 더 많이 변경되었음을 보여줍니다. 그 이유는 DDoS 공격 이벤트가 발생하면 DPS 공급자가 피해자에게 속한 접두사를 알리고 트래픽을 스크럽하기 때문입니다.

3 System Design

그림 2는 조사 프로세스의 개요를 보여줍니다. 교육 단계와 모니터링 단계로 구성됩니다. 두 단계 모두 고정된 시간 간격 내에 BGP 업데이트 데이터에서 여러 기능을 추출합니다. 추출된 특징을 벡터로 그룹화하며, 이 문서의 나머지 부분에서는 이를 데이터 빈(databin)이라고 합니다. DDoS 공격이 식별되면 DPS의 AS에서 시작된 BGP 업데이트 트래픽은 완화 정책 분석 모듈에서 추가로 분석됩니다. Intel(R) CUP Q9550 @2.83GH 및 8.0GB RAM이 있는 64비트 Windows 10 시스템에서 실행되는 Python을 사용하여 시스템의 프로토타입을 개발합니다.

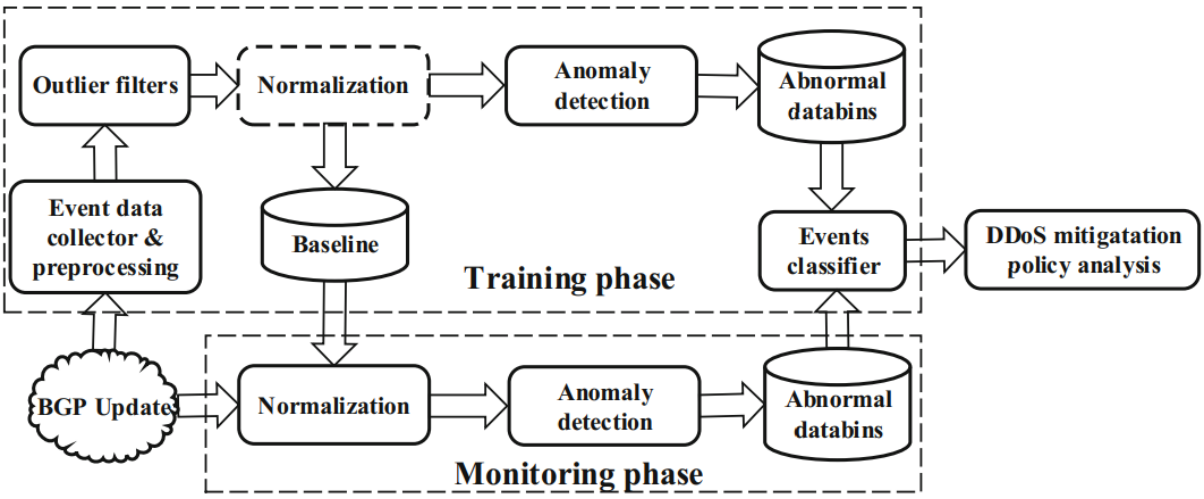

그림 2. 시스템의 아키텍처

3.1 Training Phase

먼저 허리케인, 정전, 지진, 케이블 단선, DDoS 공격 등 BGP 변경을 유발하는 다양한 종류의 이벤트를 수집합니다. 이러한 이벤트의 발생 시간을 확인하기 위해 이러한 이벤트에 대한 관련 뉴스를 수동으로 검색했습니다. 교육 단계에서는 이러한 이벤트의 발생을 다루는 기간 동안 BGP 업데이트 데이터를 수집합니다. BGP 트래픽은 본질적으로 동적이며 정상 상태에서도 일부 이상값이 있기 때문에 k-means 방법을 사용하여 정상 기간의 이상값 데이터 빈을 필터링합니다[12]. 특히, 정상 기간의 데이터 빈은 유클리드 거리에 따라 두 그룹으로 군집화됩니다. 대다수 그룹은 일반 데이터 빈만 포함할 것으로 예상되며 정규성의 기준으로 사용됩니다. 발생 기간에 대부분의 일반 데이터 빈이 포함되도록 하기 위해 일반 데이터 빈을 발생 기간의 데이터 빈과 혼합합니다. 다시 k-means 방법을 사용하여 혼합 데이터 빈을 두 그룹으로 클러스터링합니다. 대다수 중 한 명은 정상으로, 다른 한 명은 비정상으로 차별받는다. 연속적인 비정상 데이터 빈을 얻기 위한 타임스탬프에 따라 얻은 비정상 데이터 빈을 추가로 그룹화합니다. 이러한 연속적인 비정상 데이터 빈은 (1) 간격이 3분 미만이고 (2) 클러스터에 3개 이상의 연속 데이터 빈이 있는 두 가지 요구 사항을 충족합니다. 연속적인 비정상 데이터 빈의 획득된 그룹을 "인시던트"라고 합니다.

둘째, 인시던트 유형에 수동으로 레이블을 지정합니다. 이 백서에서는 재해 이벤트와 DDoS 공격만 구분합니다. 41개의 역사적 사건을 수집하고 사건 유형에 수동으로 레이블을 지정합니다. 결과는 표 2에 요약되어 있으며 이러한 이벤트를 사용하여 랜덤 포레스트 방법의 분류 모델을 학습합니다. 재해 이벤트와 DDoS 공격 이벤트만 구분합니다. 우리는 시스템의 정확도를 평가하기 위해 5 겹 교차 검증 방법을 사용합니다. 각 카테고리에서 감지된 비정상 데이터 빈은 5개의 접기로 나뉘며 각 테스트에서 5개의 접기 중 하나를 테스트 데이터로, 나머지 4개의 접기를 학습 데이터로 사용합니다. 결과는 5개 결과의 평균을 구하여 얻을 수 있습니다. 수집된 데이터를 기반으로 91.2%의 정확도를 얻었습니다.

표 2. Data set 요약

Type	Event number	Detected databins
Hurricane	4	30
Black out	4	14
Earthquake	4	152
Cable cut	9	602
DDoS	20	889

3.2 Monitoring Phase

모니터링 단계에서 새로 수집된 BGP 업데이트 메시지는 교육 단계에서 얻은 기준을 사용하여 표준화됩니다. 보다 정확하게는 이 논문에서는 Z-점수 정규화 방법을 사용하여 데이터 빈을 정규화합니다. 특징의 Z-점수 값은 z = x−μ σ로 계산되며, 여기서 μ는 구한 정규 데이터 빈의 평균이고 σ는 표준 편차입니다. 계산된 평균과 편차는 모니터링 단계에서 데이터 빈을 정규화하는 데 사용됩니다. 이상 탐지 모듈은 BGP 역학에 이상이 있는지 여부를 탐지합니다. 이상 징후가 감지되면 시스템은 훈련된 분류자를 활용하여 비정상적인 이벤트가 DDoS 공격으로 인한 것인지 여부를 식별합니다.

이 시스템을 통해 실무자가 자신의 경험 지식을 활용하여 시스템의 성능을 향상시킬 수 있다는 점은 주목할 가치가 있습니다. 경보가 울리면 실무자는 다른 외부 정보 소스를 기반으로 결과에 대한 판단을 내릴 수 있습니다. 예측이 실무자의 판단과 일치하면 새로 들어오는 데이터 빈이 학습 데이터 빈에 추가됩니다. 그렇지 않으면 예측이 거부됩니다.

3.3 Mitigation Policy Analysis

DPS에서 사용하는 BGP 기반 완화 정책을 분석하는 모듈을 제공합니다. DDoS 이벤트가 확인되면 이 모듈을 사용하여 DPS에서 채택한 BGP 정책을 검사합니다. 실무자가 자신의 경험과 지식을 활용하여 시스템의 성능을 향상시킬 수 있다는 점은 주목할 가치가 있습니다. 경보가 울리면 의사는 다른 외부 정보 소스를 기반으로 결과에 대한 판단을 내릴 수 있습니다. 예측이 실무자의 판단과 일치하면 새로 들어오는 데이터 빈이 학습 데이터 빈에 추가됩니다. 그렇지 않으면 예측이 거부됩니다.

DPS 공급자가 채택한 정책을 자동으로 추출하는 알고리즘을 개발합니다. DPS 공급자는 고객이 DDoS 공격을 받고 있음을 발견하면 BGP 사전 추가를 수행할 수 있습니다. Prefixing은 AS 경로의 왼쪽에 하나 이상의 AS 번호를 추가하는 것을 의미합니다. 일반적으로 이 작업은 자신의 AS 번호

를 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 B0이라고 합니다. 접두사 작업에서 ASN은 BGP 라우팅 경로에 나타나고 WADup BGP 업데이트 메시지는 AW BGP 업데이트 메시지를 따릅니다. 직접 보호 작업은 DPS 공급자의 ASN이 BGP 라우팅 경로의 첫 번째 홉 역할을 하는 작업으로 정의되며, AADiff BGP 업데이트 메시지는 AADiff BGP 업데이트 메시지를 따릅니다. 선행 작업을 B1로, 지시된 보호 작업을 B2로 표시합니다. 알고리즘은 다음과 같이 작동합니다. 먼저 각 희생자 접두사에 대해 AW, WWDup, AADupType1, AADupType2, AADiff, WADup, WADiff 태그를 사용하여 BGP 업데이트 레코드에 레이블을 지정합니다. BGP 업데이트 메시지에 레이블을 지정한 후 피해자를 보호하기 위해 DPS 공급자가 채택한 정책을 반영하는 B0, B1 및 B2 시퀀스를 인식합니다.

4 Experiment

4.1 Evaluation of DDoS Attack Detection

우리 시스템은 2016년 10월에 Dyn에 대한 DDoS 공격을 탐지하는 데 성공했습니다[8]. 2016년 10월 21일, Dyn은 관리되는 DNS 네트워크의 기능을 사용하는 방대한 클라이언트의 DNS 쿼리로 인해 어려움을 겪습니다. 이로 인해 Dyn의 DNS 서비스를 사용할 수 없게 되었습니다. 이로 인해 수많은 웹 사이트를 연결하는 데 어려움이 있습니다. 공격이 진행되는 동안 다른 DNS 공급자로 이동하는 트래픽이 급격히 증가하여 네트워크 트래픽이 광범위하게 정체되었습니다. 이러한 정체로 인해 결국 BGP 트래픽의 비정상적인 역학이 발생하며, 이를 통해 BGP 역학을 통해 Dyn DDoS 공격 이벤트를 탐지할 수 있습니다.

그림 3은 시간 대비 영향 값을 보여 줍니다. 정규화된 피처와 기준선 간의 차이의 합계인 영향 값은 데이터 빈과 일반 데이터 빈의 거리를 나타냅니다. 2016년 10월 21일, 비정상 역학의 세 가지 주기가 세 개의 빨간색 블록으로 설명됩니다. 당사의 이상 탐지 모듈은 이러한 비정상적인 데이터 빈을 식별하고 DDoS 공격으로 올바르게 분류할 수 있습니다. 감지된 비정상 기간은 다음과 같이 설명됩니다.

– 첫 번째 기간은 04:30:22(PDT)에 시작되었으며 BGP 트래픽의 변동이 시작되었습니다. 06:16:00 (PDT) 경까지 변동은 줄어들었습니다. 이는 보고된 인시던트의 시작 및 완화 시간과 일치합니다[18]. 이 기간 동안 아시아 태평양 및 동유럽에 있는 Dyn의 DNS 서버 플랫폼은 대규모 요청과 미국 동부 지역으로 인해 방대한 BGP 경로 역학을 초래했습니다[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].

– 우리 시스템은 또한 13:19:28에 시작하여 약 14:08:0(PDT)에 종료된 비정상적인 BGP 역학의 세 번째 기간을 감지했습니다. 이는 뉴스에 보도된 DDoS 공격 기간과도 일치합니다[8].

또한 그림 3과 같이 녹색 블록이 있는 BGP 트래픽에서 각각 01:22:23(PDT) 및 17:47:1에 시작된 몇 가지 명백한 변동이 추가로 발견되었습니다. 그러나 이러한 사건은 Dyn.com 또는 기타 뉴스 매체에 의해 보도되지 않습니다. 이러한 사건은 DDoS 공격의 시작과 여진으로 인해 발생한 것으로 추측됩니다(표 3).

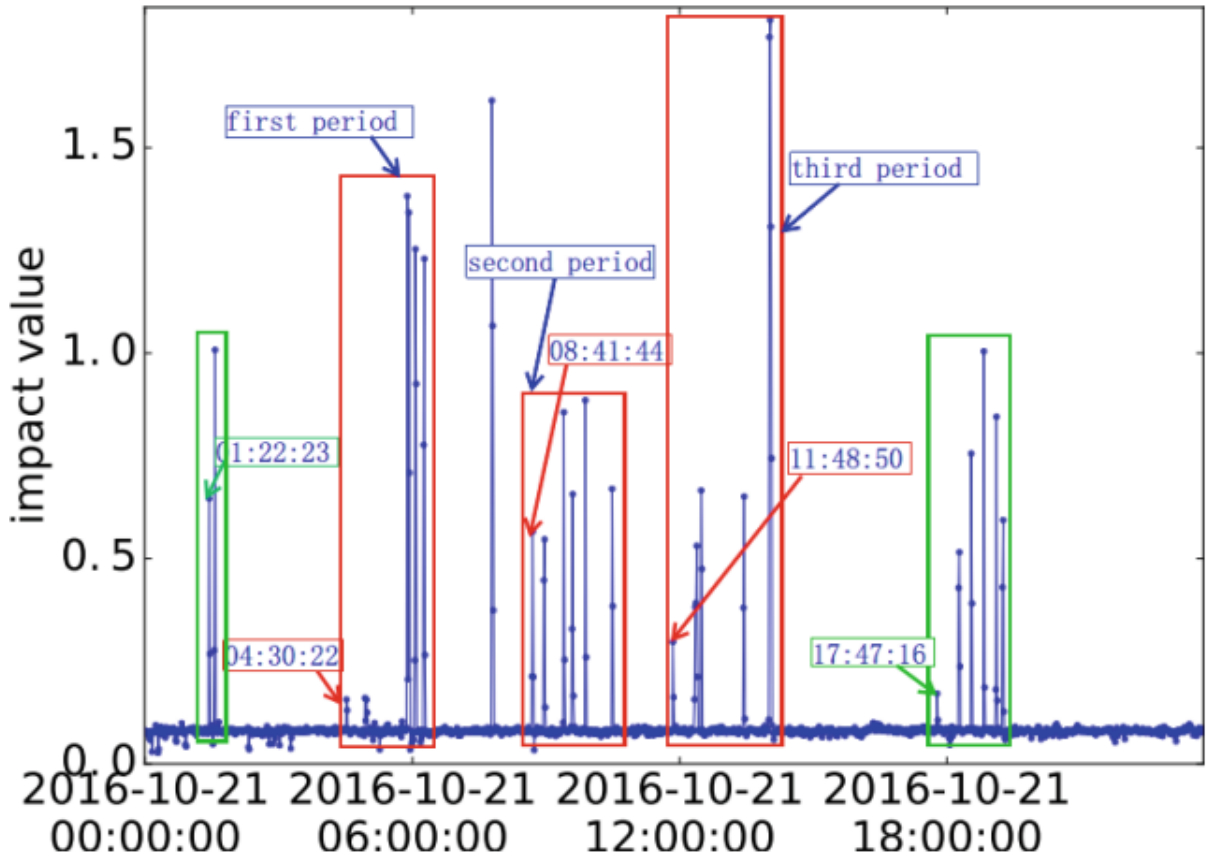

Fig. 3. Dyn DDoS attack overview

5 Related Work

많은 연구에서 BGP 역학의 불안정성 또는 병리학적 동작 감지를 다루었습니다. Labovitz et al. [11]은 BGP 라우팅 메시지를 조사한 결과 라우팅 업데이트 볼륨이 예상보다 더 중복되는 것을 발견했습니다.

표 3. 세 prefix의 업데이트 패턴 시퀀스에 대한 DPS 보호 동작

Prefix	Update pattern sequence
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 포워딩 불안정성과 라우팅 정책 변동의 예상치 못한 몇 가지 추세를 드러냈습니다. Deshpande 등[6]은 통계적 패턴 인식 기술을 적용하여 GBP 역학의 불안정성을 감지하는 온라인 불안정성 감지 아키텍처를 제안했습니다. 그들은 AS 경로 길이 및 AS 경로 편집 거리와 같은 기능이 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 et al. [7]은 BGP 업데이트에서 라우팅 불안정의 원인을 식별하는 방법론을 제안했습니다. 여러 연구에서 통계적 패턴 인식 기술을 활용하여 BGP 라우팅 역학의 불안정성을 감지합니다[6,11,13]. 이러한 연구와 비교하여 본 논문에서는 비정상적인 BGP 역학의 두 가지 주요 원인인 DDoS 공격 이벤트와 파괴적인 재해 이벤트를 구별하는 기계 학습 기반 방법을 제안합니다. 이를 통해 BGP 트래픽 이상이 탐지될 때 DDoS 공격이 진행 중인지 여부를 식별할 수 있습니다.

정전, 케이블 절단, 웜 및 접두사 하이재킹 공격 등과 같은 역사적 사건이 가져온 영향을 분석하여 많은 후향적 연구가 수행되었습니다. Cowie 등[5]은 2001년 7월과 9월에 각각 발생한 Code Red II 및 Nimda 웜으로 인한 글로벌 BGP 라우팅 불안정을 분석했습니다. 그 결과, 정전 지역에서 공개적으로 드러난 것보다 그 영향이 더 심각하다는 것을 발견했다. Li et al. [14]은 글로벌 및 접두사 수준의 관점에서 대규모 정전 시 BGP 동작을 분석했습니다. 그들은 전 세계적으로 인출 건수가 증가했음을 발견했습니다. 결과적으로, 접두사 수준에서 에지와 노드의 수가 급격히 감소했습니다. 이러한 연구는 주로 중단 이벤트가 BGP 라우팅의 성능에 미치는 영향에 관한 것입니다. 이 백서에서는 DDoS 공격으로 인한 중단과 다양한 DPS 정책의 영향에 중점을 둡니다.

6 Conclusion

이 백서에서는 BGP 기반 DDoS 보호 서비스의 동작을 조사합니다. 지진, 정전, 케이블 절단 등과 같은 다른 파괴적인 이벤트가 아닌 DDoS 공격으로 인한 비정상적인 BGP 역학을 식별하기 위해 BGP 역학의 비정상적인 동작을 유발하는 것으로 입증된 40개 이상의 수동으로 수집된 이벤트 데이터 세트를 기반으로 적절한 분류자를 훈련합니다. 또한 비정상적인 BGP 업데이트 메시지를 통해 DDoS 이벤트를 탐지하는 시스템을 개발하고 일반적인 DDoS 공격에 대한 DPS의 동작을 분석하는 새로운 알고리즘을 설계합니다. 실제 DDoS 공격에 시스템을 적용하여 DPS가 공격을 완화하는 데 사용하는 정책을 식별하고 몇 가지 의미 있는 결과를 얻을 수 있습니다. 이 연구는 효과적인 DDoS 공격 완화 체계의 설계에 대해 설명합니다.

References

1. How friday's massive ddos attack on the U.S. happened. https://en.wikipedia.org/ wiki/2016 Dyn cyberattackcite note-wired-5/

2. OVH suffers from 1.1Tbps DDoS attack. https://www.scmagazineuk.com/ovh□suffers-11tbps-ddos-attack/article/532197/. Accessed 11 Mar 2017

3. Chandrashekar, J., Duan, Z., Zhang, Z.L., Krasky, J.: Limiting path exploration in BGP. In: 24th

Annual Joint Conference of INFOCOM, vol. 4, pp. 2337–2348. IEEE (2005)

4. Chang, D.F., Govindan, R., Heidemann, J.: The temporal and topological characteristics of BGP path changes. In: ICNP, pp. 190–199. IEEE (2003)

5. Cowie, J., Ogielski, A.T., Premore, B., Yuan, Y.: Internet worms and global routing instabilities. In: ITCom 2002: The Convergence of Information Technologies and Communications, pp. 195–199 (2002)

6. Deshpande, S., Thottan, M., Ho, T.K., Sikdar, B.: An online mechanism for BGP instability detection and analysis. IEEE Trans. Comput. 58(11), 1470–1484 (2009)

7. Feldmann, A., Maennel, O., Mao, Z.M., Berger, A., Maggs, B.: Locating internet routing instabilities. ACM SIGCOMM CCR 34, 205–218 (2004)

8. Hilton, S.: Dyn analysis summary of friday october 21 attack. 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.: Measuring the adoption of DDoS protection services. In: Proceedings of the 2016 ACM on Internet Measurement Conference, pp. 279–285. ACM (2016)

10. Karami, M., McCoy, D.: Understanding the emerging threat of DDoS-as-a-service. In: LEET (2013) 11. Labovitz, C., Malan, G.R., Jahanian, F.: Internet routing instability. IEEE/ACM Trans. Netw. 6(5), 515–528 (1998)

12. Li, J., Brooks, S.: I-seismograph: observing and measuring internet earthquakes. In: INFOCOM, 2011 Proceedings IEEE, pp. 2624–2632. IEEE (2011)

13. Li, J., Guidero, M., Wu, Z., Purpus, E., Ehrenkranz, T.: BGP routing dynamics revisited. ACM SIGCOMM CCR 37(2), 5–16 (2007)

14. Li, J., Wu, Z., Purpus, E.: Cam04-5: Toward understanding the behavior of BGP during large-scale power outages. In: IEEE Globecom. IEEE (2006)

15. Noroozian, A., Korczy´nski, M., Ga˜nan, C.H., Makita, D., Yoshioka, K., van Eeten, M.: Who gets the boot? analyzing victimization by DDoS-as-a-service. In: Monrose, F., Dacier, M., Blanc, G., Garcia-Alfaro, J. (eds.) RAID 2016. LNCS, vol. 9854, pp. 368–389. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-45719-2 17 Understanding the Behaviors of BGP-based DDoS Protection Services 473

16. Park, J.H., Jen, D., Lad, M., Amante, S., McPherson, D., Zhang, L.: Investigating occurrence of duplicate updates in BGP announcements. In: Krishnamurthy, A., Plattner, B. (eds.) PAM 2010. LNCS,

vol. 6032, pp. 11–20. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-12334-4 2

17. Santanna, J.J., et al.: Booters-an analysis of DDoS-as-a-service attacks. In: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 243–251. IEEE (2015)

18. Smith, D.: How friday's massive ddos attack on the U.S. happened. https://blog. radware.com/security/2016/10/fridays-massive-ddos-attack-u-s-happened/ 19. Zhang, M.: BGPInspector: A real-time extensible border gateway protocol moni□toring framework. CAS (2014