지도환 - Understanding the Behaviors of BGP-based DDoS Protection Services

Abstract

DPS(DDoS protection services)의 일반적인 방법 중 하나

- BGP 정책들의 변경을 통한 트래픽 경로 재 지정
  but, Abnormal BGP routing dynamics 야기 가능성 존재.

Abnormal BGP routing dynamics : 라우팅 경로의 급격한 변화, 라우팅 불안정성 증가 또는 네트워크 트래픽의 정상적인 흐름의 중단과 같은 비정상적이거나 예상치 못한 동작

하지만 이 행동에 대한 결과는 알려져 있지 않음.

위 문제를 해결하기위해 BGP 기반 DPS의 동작에 대한 연구 진행

1. 실제 DDoS 사건들을 식별하기 위한 machine learning 기반 접근 방식 제안
   실제 DDoS 사건들을 특성화하기 위한 데이터가 보통 부족하기 때문
2. 전형적인 DDoS 공격들에 대한 DPS의 행동을 분석한 새로운 알고리즘 설계

1 Introduction

DDoS는 오래전부터 위협해옴.

DDoS-as-a-service economy, 1Tbps 이상의 DDoS 공격이 나타나서 더 위험함. 이는 막대한 금전적 손실을 입을 수도 있음.

그래서 트래픽 전환 방식의 DPS 시장 급성장 중.

트래픽 전환은 상시 또는 요구에 따라 DPS 인프라를 통해 트래픽을 라우팅 가능.

방식

- DNS 기반
  Domain Name Serves 또는 Anycast 기술들의 적절한 사용을 통해 트래픽 분산
  CDN 방식과 유사
- BGP 기반
  BGP 기반 체계는 고객의 IP 서브넷을 공지함으로써 Scrubbing을 위해 트래픽을 DPS 인프라로 전환한다. **Scrubbing** : 악의적이거나 원치 않는 트래픽을 식별하고 완화하기 위해 들어오는 네트워크 트래픽을 검사하고 필터링하는 프로세스

이 논문에선 BGP 기반 방법에 대해서 할 것임.

2 Feature Analysis

수집한 BGP 업데이트 메시지에서 특징 및 비교

Table 1. Description of features

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

Ann : BGP speakers에 의해 일반화된 announcements 수

- 3k 미만인 경우, DDoS 80%, 재해 50% 미만, 재해는 길어서 새로운 경로 발표.

WADiff : 명시적 철회 후 새로 알려진 경로 수

- 재난 발생 시가 더 많음, 일부 BGP 경로에 연결 할 수 없기 때문.

AADupType1 : 같은 IP prefix(ex. /24)에 중복된 announcements 수

- DDoS는 5~600개로 급격히 증가, 결과적으로 경로가 변경될 수록 많아짐.

Unq_pfx_as : 한 AS에서 발생한 고유 prefixes 수

- announcements와 withdrawal이 많은 경우는 보통 불안정할 때 특징, BGP 기반 DDoS 대응 방식을 사용하기 때문에, 더 불안정해 보임.

Max_AS_path_len : AS-PATHs의 최대 길이

- AS가 공격 받는 경우, 운영자는 BGP prepending을 할 수 있고, 이러면 최대 길이가 늘어남.
- DDoS는 25~30개에 집중, 재해의 경우 고르게 분포

pfx_org_chg : Prefix 변경 횟수.

- DPS가 DDoS시, scrubbing 하기 때문에, Prefix 변경 횟수가 많음.

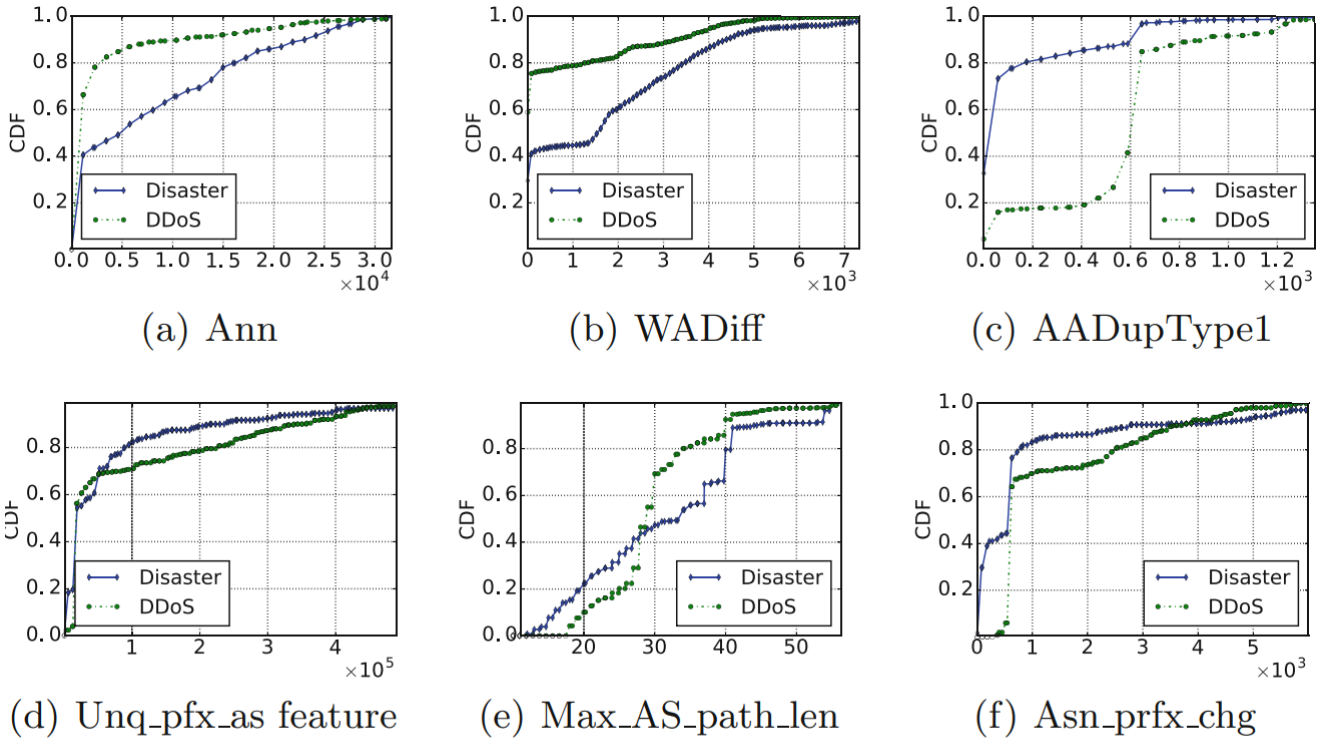

Fig. 1. CDF of the features

CDF 그래프이므로, 기울기가 곧 그 구간의 데이터가 많다는 것을 말함.

위 특성에 따른 그래프를 통해 재해와 DDoS를 구분 할 수 있음.

3 System Design

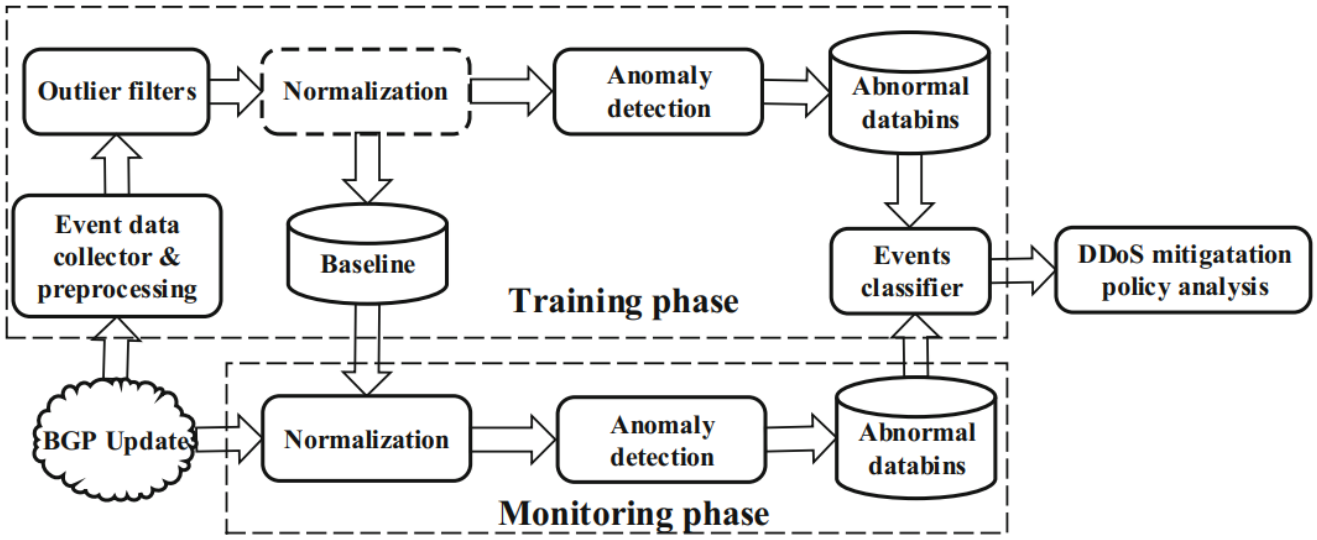

Fig. 2. The architecture of the system

3.1 Training Phase

교육할 자료를 찾기 위해, 자연 재해, 케이블 절단, DDoS 공격이 일어났던 시기를 먼저 찾아야 한다.

관련 뉴스를 찾아 시기를 찾아냄. 그리고 이때의 BGP 업데이트 데이터를 수집.

정상 상태에서도, 일부 이상 값이 존재함. 따라서, k-mean 알고리즘으로 이상 값 데이터를 걸러냄.

K-mean 알고리즘 : machine learning의 비지도 학습 중 하나로, 유클리드 거리에 기초하여 K개의 그룹으로 클러스터링(군집화)하는 것.

두 그룹으로 나누어 짐. 1. 정상, 2. 비정상

비정상은 다시 시간 기록에 따라, 1. 간격이 3분 미만, 2. 연속된 데이터 3개 이상 기준으로 걸러 “연속적인 비정상 데이터”를 얻음.

그리고 이 것에 대해 원인을 직접 라벨링을 함. 결과는 다음과 같음.

Table 2. A summary of the dataset

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

위에서 학습한 데이터로 얻은 기준선을 사용하여 BGP 업데이트 메시지를 정규화 한다.

이상 감지를 했을 때, 실무자가 판단도 동일하면 학습 데이터에 추가하여 시스템의 성능을 개선시킬 수 있고, 아니면 해당 이상 감지 예측은 버린다.

3.3 Mitigation Policy Analysis

DPS 제공업체가 채택한 정책을 자동으로 추출하는 알고리즘

DPS 제공자는 고객이 DDoS 공격을 받고 있음을 발견하면 BGP prepending을 수행할 수 있다.

BGP prepending : 경로를 알릴 때, 자기 자신을 두 번 이상 넣어 알리는 것으로, 최단 경로로 routing하는 방식에서 cost가 증가하는 결과를 야기하기 때문에, 패킷이 다른 경로를 경유하게끔 유도함.

B0 : 이러한 보호 프로세스는 WADiff BGP 업데이트 메시지로 시작, AW BGP 업데이트로 끝남.

B1 : 선행 조치에서 ASN은 BGP 라우팅 경로에 나타나고 WADup BGP 업데이트 메시지는 AW BGP 업데이트 메시지 다음에 나옴.

B2 : 직접 보호동작은 DPS 제공업체의 ASN이 BGP 라우팅 경로의 첫 번째 홉 역할을 하는 동작으로 정의하며, AADiff BGP 업데이트 메시지는 AADiff BGP 업데이트 메시지 뒤에 따라 나오게 됨.

4 Experiments

4.1 Evaluation of DDoS Attack Detection

위 시스템으로 16년 10월 Dyn에 대한 DDoS 공격을 탐지하는 데 성공.

- DNS flood DDoS Attack 발생
- 공격이 진행되는 동안 다른 DNS 공급업체로 이동하는 트래픽이 급격히 증가.
- 네트워크 트래픽이 광범위하게 혼잡해짐.
- BGP 트래픽의 비정상적인 동적 변화 초래
- DDoS 공격 이벤트 감지 가능.

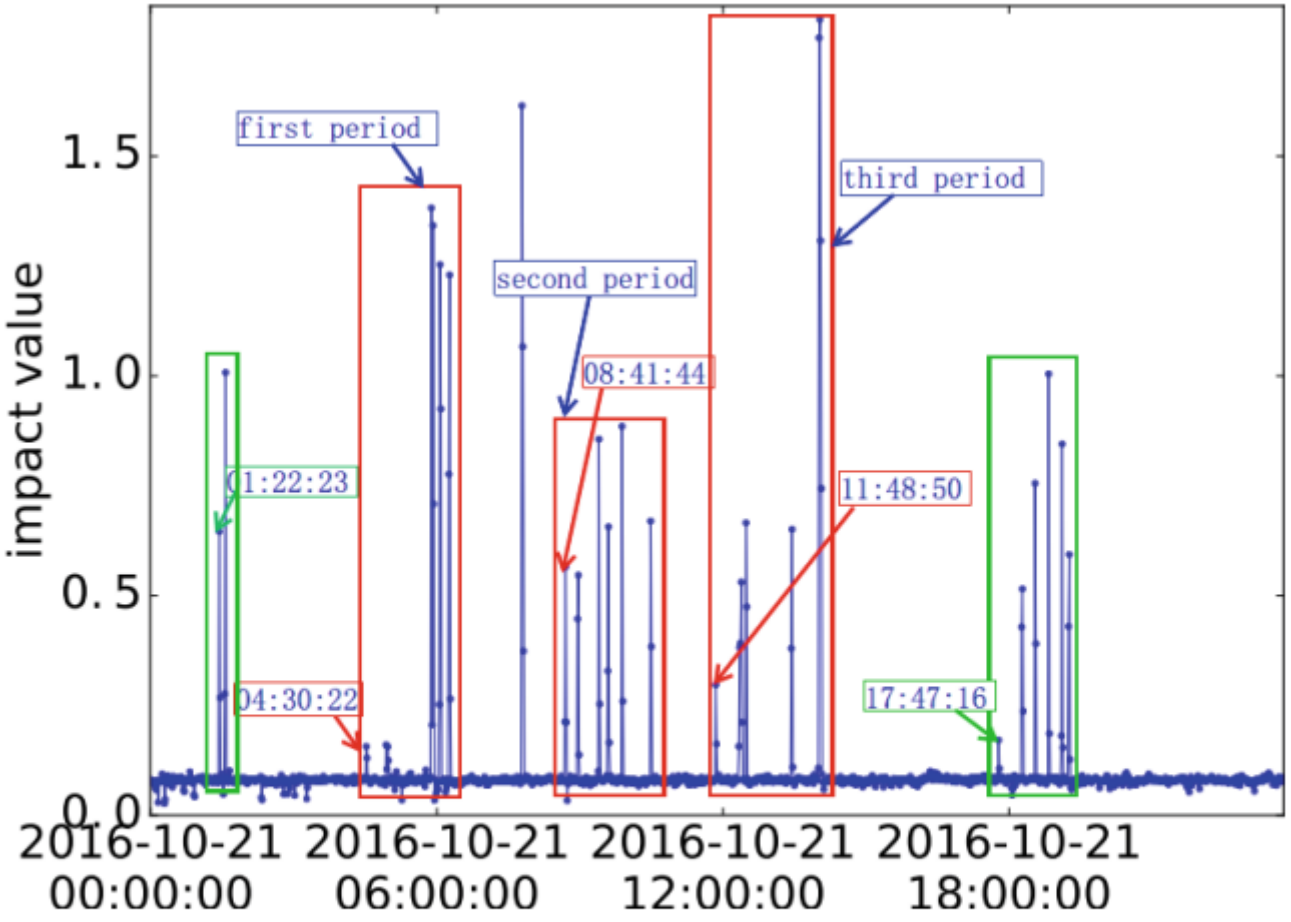

Fig. 3. Dyn DDoS attack overview

빨간색 블록은 각각 BGP 경로 변동이 발생했고, 보고되거나 뉴스 보도 내용과 공격 기간이 일치함.

초록색 블록은 보고되거나 뉴스에 보도 X, DDoS 공격의 시작과 여진에 의해 발생한 것으로 추정.

5 Related Work

Labovitz : BGP 라우팅 업데이트의 양이 예상보다 많다는 사실을 발견.

Table 3. DPS protection behaviors of update pattern sequences of three prefixs

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

- 포워딩 불안정성과 라우팅 정책 변동에 대한 몇 가지 예상치 못한 추세를 밝힘.

Deshpande : 통계적 패턴 인식 기법을 적용하여 GBP(오타?) dynamics의 불안정성을 감지하는 온라인 아키텍처 제안

Chang : BGP update stream에서 도메인 간 경로 변경 이벤트를 식별하는 알고리즘을 제안.

Feldmann : BGP 업데이트에서 라우팅 불안정성의 원인을 식별하는 방법론 제안.

- 이를 통해 BGP 트래픽 이상 징후 감지 시, DDoS 공격 여부 확인할 수 있었음.

Cowie : code read II와 님다 웜으로 인한 글로벌 BGP 라우팅 불안정성을 분석.

- 블랙아웃 지역에서 그 영향이 더 심각하다는 것을 발견.

Li : 블랙아웃 시, BGP의 행동을 글로벌 및 prefix 수준의 관점에서 분석.

- 글로 수준에서 withdraw 건수가 증가한다는 사실을 발견.
- prefix 수준에서 edge와 node 수가 급격히 감소.

6 Conclusion

- **BGP 기반 DDoS 보호 서비스의 동작을 조사함.**
- **자연 재해나 케이블 절단이 아닌 DDoS 공격으로 인한 비정상적인 BGP 역학을 식별하기 위해 BGP 역학의 비정상적인 동작을 유발하는 것으로 입증된 40개 이상의 수동 수집된 이벤트 데이터 세트를 기반으로 적절한 분류기를 훈련함.**
- **또한 비정상적인 BGP 업데이트 메시지를 통해 DDoS 이벤트를 탐지하는 시스템을 개발, 일반적인 DDoS 공격에 대한 DPS의 행동을 분석하는 새로운 알고리즘을 설계함.**
- **이 연구는 효과적인 DDoS 공격 완화 방안의 설계를 조명함.**