# Routing Around Congestion Defeating DDoS Attacks and Adverse Network Conditions via Reactive BGP Routing 🥅

<원문>

Routing Around Congestion Defeating DDoS Attacks and Adverse Network Conditions via Reactive BGP Routing 2.pdf

<번역본>

번역 - Routing Around Congestion Defeating DDoS Attacks and Adverse Network Conditions via Reactive BGP Routing.pdf

<참고 자료>

https://slideplayer.com/slide/14287264/

## 1️⃣ 기존 DDoS 방어 방법의 한계

- 기존의 DDoS 방어 방법은 주로 마지막 마일 링크를 보호하는 데 초점을 맞추고 있어 트랜짓 링크를 보호하지 않는 한계가 있습니다.

- 대부분의 DDoS 방어 방법은 공격 트래픽이 피해자에게 직접 전달되는 것을 전제로 하기 때문에, 트랜짓 링크 DDoS와 같은 새로운 형태의 공격에 취약합니다.
- 이러한 한계로 인해 공격자는 피해자의 끝단 호스트가 아닌 피해자의 외부에 위치한 공유 트랜짓 링크를 공격하는 방식을 채택하고 있으며, 이는 기존 방어 방법으로는 효과적으로 대응하기 어려운 상황을 초래하고 있습니다.

## 2️⃣ Nyx란?

Nyx는 AS 간 트래픽을 우회하고 DDoS 공격을 처리하는 기술로, AS 간 연결성을 제한하지 않고 다른 AS에서의 BGP 광고를 줄이지 않으면서 공격 트래픽을 관리합니다. Nyx는 AS 간 경로 조작을 통해 공격 트래픽을 무시하고 혼잡한 경로를 피할 수 있도록 설계되었습니다. 이 기술은 AS 간 경로 선택을 통해 효과적인 트래픽 분리를 달성하며, 외부 협력 없이 단일 다중 연결 AS에 배포될 수 있습니다.

## 3️⃣ Nyx의 특징

1. **FRRP 기술 활용**: Nyx는 FRRP를 통해 거짓 경로를 생성하고 관리함으로써 네트워크 트래픽을 조작합니다. 이를 통해 공격에 의해 영향을 받는 링크를 우회하고 네트워크 성능을 최적화할 수 있습니다.
2. **네트워크 혼잡 완화**: Nyx는 검색 알고리즘을 활용하여 혼잡한 링크를 피해 최적의 경로를 탐색합니다. 이를 통해 DDoS 공격으로 인한 네트워크 혼잡을 완화할 수 있습니다.
3. **강건성 및 유연성**: Nyx는 다양한 DDoS 공격 모델과 매개변수에 대응할 수 있는 강건성을 갖고 있다. 공격의 강도나 유형에 관계없이 안정적인 성능을 제공합니다.

## 4️⃣ Nyx 성능 분석

- Nyx는 DDoS 공격에 강건하고 유연한 성능을 제공합니다. 이 시스템은 공격을 받은 링크를 우회하고 DDoS 공격으로 인한 혼잡을 완화하기 위해 네트워크 트래픽을 조작하고 최적 경로를 탐색하여 네트워크 성능을 최적화합니다.
- Nyx는 다양한 공격 모델과 매개변수에 대응하여 네트워크 보안을 강화하며, 트랜짓 링크와 마일 링크를 보호하는 데 초점을 맞추어 효과적인 방어 기능을 제공합니다.
- 시뮬레이션 결과에 따르면 Nyx는 공격 강도에 민감하지 않으며, 단일 AS에 배포되어 외부 협력 없이도 효과적으로 운영될 수 있음을 보여줍니다.

## 5️⃣ Nyx의 장점 및 활용방안

- Nyx는 AS 간 트래픽을 우회하고 DDoS 공격을 처리하는 데 사용되므로 네트워크 보안을 강화하는 데 활용할 수 있습니다.
- FRRP 기술을 활용하여 네트워크 트래픽을 조작하고 혼잡한 링크를 우회함으로써 성능을 최적화할 수 있어 네트워크 성능 향상에 활용될 수 있습니다.
- 다양한 DDoS 공격 모델과 매개변수에 대응할 수 있는 강건성과 유연성을 갖고 있어 다양한 네트워크 환경에서 효과적으로 활용할 수 있습니다.

## 6️⃣ Nyx가 필요로 하는 정보

| Information Needed | How Nyx Uses Information | Information Source |
|---|---|---|
| Critical AS | Traffic from Critical AS moved around degraded or attacked links | Chosen by Deployer AS |
| Paths between Deployer AS and Critical AS | Alternate, non-degraded paths between Critical AS and Deployer AS chosen based on any known paths | Deployer BGP speaker's Routing Information Base (RIB) |
| ASes bordering alternate paths between Deployer AS and Critical AS | BGP loop detection is used during FRRP to reduce disturbance by appending ASes bordering alternate paths | Deployer BGP speaker's Routing Information Base (RIB) |

TABLE I: Information Needed by Nyx

- **AS와 AS 간의 트래픽 이동**
  - Critical AS와 Deployer AS 간의 트래픽은 손상된 경로나 대체 경로를 통해 이동합니다.
- **BGP 루프 감지**
  - 루프 감지를 통해 AS 간의 불필요한 경로를 제거합니다.
- **정보 필요성**

- Deployer AS가 선택한 경로는 BGP 스피커의 라우팅 정보 베이스에 의해 결정합니다.

7️⃣ Nyx가 필요로 하지 않는 정보

| Information Not Needed | How Nyx Works Without |
|---|---|
| Bandwidth/Capacity of links in the Internet | Nyx does not need to know the bandwidth of links, it only measures it's success by the ratio of critical traffic sent to what is actually received by the Deployer AS |
| Location of malicious bots and botnets in the Internet | Nyx does not need to know where bots live, since Nyx will continue searching for alternate, non-degraded paths until the least degraded path is found, ignoring what networks are actually sending attack traffic |
| Malicious and benign traffic | Nyx does not need to know what traffic is malicious, we only need to know what Critical AS is trying to establish a non-degraded path to us, and we consider the traffic from the Critical AS as "benign" |

- Nyx는 악성 봇의 대역폭이나 위치를 알 필요가 없습니다.
- Nyx는 비정상적인 트래픽이 아닌 Critical AS의 트래픽을 고려하여 경로를 설정합니다.
- Nyx는 최소한의 손상된 경로를 찾을 때까지 대체 경로를 탐색합니다.