※ 본 양식은 평가항목을 기반으로 작성되었으며, 양식에 주어진 기본항목은 변경 가능합니다.

소 속	울산대학교
팀 명	가보는거야
팀 원	김영일
제출 일자	2023.10.20

□ 서론

1. 최근 이슈 및 아이디어 요약 등 서론 내용

최근 북한 7.7 디도스 공격의 주역인 김영철 당중앙위원회 통일전선부 고문이 일선으로 복직시켰으며, 출신성분을 가리지 않고 해커를 양성하기 시작하고 있다. 그 결과 북한의 사이버전 역량은 점점 강해지고 있으며, 심지어 최근 해커어스에서 주최한 해킹 대회에서 북한 대학생 팀이 우승을 차지하는 등 그 실질적인 위협이 점점 심화하고 있다.

그리고 실제로 이슈메이커랩스의 조사에 따르면, 2004년에 비해서 2021년에는 북한의 대한민국을 겨냥한 사이버 공격이 약 300배가 증가한 모습을 보인다고 발표[1] 했으며, 그 공격은 랜섬웨어, DDoS, 랜섬 디도스 등 그 공격 방법은 점점 다양해지고 있다.

그 중 특히 대규모 트래픽을 이용한 DDoS 공격은 7.7 DDoS 사태 이후 꾸준히 국내 정부, 기관, 기업들을 대상으로 많이 이루어지고 있는데, 이런 DDoS 공격을 탐지하기 위해 우리는 주로 임곗값을 이용한 이상치 탐지, IP 필터링, 그리고 최근에는 머신러닝을 이용한 이상치 탐지 및 분류가 주로 이용된다.

하지만 최근 그 공격 대상이 국내 정부 기관, 대기업에서 상대적으로 사이버 보안이 취약한 중견 이하의 기업들을 대상으로 많이 확대되고 있다. 이에 따라 중소기업의 사이버 보안 대응 능력은 큰 기업이나 정부 기관에 비해 상대적으로 매우 취약해, 이런 사이버 공격에 표적이 되고 있다. 특히 빠른 대응이 가장 중요한 DDoS 공격의 경우, 대응 시간이 평균적으로 대기업은 3분, 중소기업은 9분[2]으로, 중소기업은 DDoS 공격에 매우 취약하다. 하지만 중소기업의 사이버 보안 인력 부족 현상이 과속화 됨에 따라 지금까지의 공격 이후 사후 대응 전략은 중소기업들에는 더욱 어려운 과제로 남아있다. 따라서 이런 중소기업들은 DDoS 공격을 사후에 대응하기보다 사전에 트래픽을 미리 파악해 DDoS 공격을 예상하고 대응하는 전략을 추가해야 한다.

이런 시계열을 이용한 트래픽 예측 및 탐지는 이미 많은 연구가 활발히 이루어지고 있는 분야 중 하나다. 특히 LSTM을 이용해 트래픽을 예측하는 "Traffic Flow Forecast through Time Series Analysis Based on Deep Learning (Zheng & Huang, 2017)", ARIMA을 비롯한 여러 통계 모델을 이용하는 "시계열 모형을 이용한 통신망 트래픽 예측 기법연구 (김삼용, 2007)" 등 많은 분야에서 연구가 이루어지고 있다. 하지만 LSTM, ARIMA 등 같은 고전적인 시계열 모델들은 여러 한계가 존재해 그 실용성이 떨어진다.

첫째, 긴 시간의 시계열 예측 및 탐지가 어렵다. 최근 사이버 공격 방식은 점점 APT 공격 방식처럼 긴 시간 동안 표적을 집요하게 공격하는 방법이 주류를 이룬다. 따라서 단기간의 예측이 아닌 장기간의 예측이 가능한 예측 모델을 사용해야 한다.

두번째, 시계열의 비정형성을 극복하지 못했다. 비정형성(nonstationarity)이란 시계열 데이

1) 권준, "북한 추정 사이버공격, "2004년부터 2021년까지 300배 이상 증가했다", 보안 뉴스, 2022-05-09, https://www.boannews.com/media/view.asp?idx=106606
2) 김민경, "디도스 공격 탐지 시간, 대기업 3분·중소기업 9분", KBS, 2021-07-06, https://news.kbs.co.kr/news/pc/view/view.do?ncd=5226505

터의 통계적 특성이 시간에 따라 일정하지 않고 변화하는 성질을 이야기하는데, 이런 고전적인 시계열 모델들은 정형성이 보장된 상황을 전제로 예측한다. 하지만 최근 산업이 급격하게 발전하면서 트래픽 수요의 변동이 이전과는 비교할 수 없을 만큼 커지게 되었고 데이터의 비정형성 역시 점점 커지면서, 이런 고전적인 시계열 모델은 현실 세계의 트래픽 예측 및 탐지에 적합한 방법이 아니다.

따라서 이런 시계열 트래픽 데이터를 통해 디도스를 탐지 및 예측하기 위해서 우리는 긴 시계열을 예측할 수 있어야 하며, 시계열의 비정형성을 극복할 수 있어야 한다. 그 결과 이번 공모전에서 "Long term 5G network traffic forecasting via modeling non-stationarity with deep learning" 모델에서 소개한 Diviner 모델을 기반으로 긴 시계열 예측과 비정형성을 극복해 DDoS를 탐지 및 예측하는 방법을 소개하려고 한다.

□ 관련 동향

1.1 *기술적 동향*

특정 시간대, 특정일 날 급증하는 트래픽을 예측하는 연구는 DDoS 탐지 등 보안 분야뿐만 아니라 네트워크 모니터링, QoS 등 여러 분야에서 연구가 이루어지고 있다. 하지만 그 기반은 시계열 예측에 두어 크게 고전적인 통계 모델을 이용하는 방식, 신경망을 기반으로 하는 방식, 트랜스포머를 기반으로 하는 방식으로 나누어지는데, 대표적인 논문들과 함께 각 방법에 대해서 소개하겠다.

1.1.1. 고전적인 통계모델

주로 ARIMA 등 고전적인 통계학의 모델을 사용하면서 예측을 진행하는 연구 방식이다. "시계열 모형을 이용한 통신망 트래픽 예측 기법연구(김상용, 2007)" 등에서 진행한 것처럼 AR, ARCH, GARCH 등 다양한 통계 모델을 활용하여 예측을 수행하는데, 보통 ARIMA 모델에서 파생된 여러 모델을 사용해서 예측을 수행하는 방식으로 진행된다. 여러 도메인에 사용되지만 및 분류 등 다른 방법으로 사용되기보다는 단순히 수식적인 예측에 좀 더 집중하는 방법이다.

1.1.2. 신경망 및 머신러닝 예측 모델

신경망 및 머신러닝 방법은 앞에서 진행한 ARIMA 등 통계모델에 비해서 예측 성능을 많이 상승시켰기 때문에, 여러 도메인에서 다양한 모델들이 적용되고 있다. 특히 "Traffic Flow Forecast through Time Series Analysis Based on Deep Learning (Zheng & Huang, 2017)" 등 여러 논문에서 RNN 모델을 활용하거나 이를 이용한 LSTM, GRU 모델들을 많이 활용한다. 그리고 이제는 이런 단순 예측뿐만 아니라 AUTOENCODER, VAE 등 비지도 학습 모델을

사용 해하거나 "IoT 네트워크에서 악성 트래픽을 탐지하기 위한 머신러닝 알고리즘의 성능 비교연구(현미진, 2021)"처럼 Lgbm, Rf 등 모델을 사용해서 이상치를 탐지하는 방식으로 트래픽 분석에 적용되고 있다.

하지만 RNN 모델은 Self-Feedback 방식으로 학습하기 때문에, 각 타임스탬프 간의 시간의 존성이 매우 강하며, 이는 장기간의 시계열을 예측하는데 매우 취약하다. 이를 극복하기 위해 LSTM, GRU 등 여러 모델이 제안되었지만, 여전히 장기간의 시계열에는 취약하며 시간의 정형성을 전제로 한다. 그리고 비지도 학습을 이용한 모델 역시 시간성을 사용하는 것이 아니라 정상인 데이터 범주에서 단순히 벗어나는 트래픽을 탐지하는 방법이 사용되고 있다.

1.1.3. 트랜스포머 예측 모델

트랜스포머 모델은 "Attention Is All You Need(Vaswani, 2017)" 논문을 시작으로 제시된 모델로, Self-Feedback을 기반으로 하는 RNN 모델과 다르게 트랜스포머 모델은 어탠션 메커니즘을 기반으로 학습을 진행해, RNN 모델의 장기간 의존성 문제를 해결 및 장기간 예측에 적절한 모델이다. 그리고 장기간의 예측뿐만 아니라 순차적으로 타임스탬프를 처리하는 RNN 모델과 달리 병렬처리를 지원하면서 속도 역시 트랜스포머 모델이 RNN 모델보다 빠르다.

1.2 *정책동향*

최근 통계에 따르면 국내 중소기업을 노린 디도스 공격이 지난 12년간 약 1400건, 최근 4년 연속으로 연간 세 자릿수 이상 발생한 것으로 나타나면서 상대적으로 사이버 보안이 취약한 중소기업들이 해커들의 표적이 되고 있다는 것을 알 수 있다. 따라서 KISA는 이에 대응해서 기업들이 DDoS로부터 대비할 수 있도록 디도스 사이버 공격 대피소 등 여러 정책들과 방법들을 제시하고 있다.

1.2.1. 디도스 사이버 공격 대피소

디도스 사이버 공격 대피소란 피해 웹사이트로 향하는 DDoS 트래픽을 대피소로 우회하여 분석, 차단함으로써 정상적으로 운영될 수 있도록 하는 KISA의 중소기업 무료 지원 서비스다. 실제로 기업에서 디도스 공격 발생을 알리면 해당 공격 트래픽을 대규모 트래픽 저장소로 보내서 공격을 우회하는 방법이다.

하지만 사전에 웹사이트를 등록하지 못하면 공격 직후 구두로 정보를 확인하고, 대피소로 등록하는 등 오랜 시간이 걸리며, 사전에 등록했다고 하더라도 공격을 탐지하고 서비스 적용을 신청해야 한다는 점, 그리고 평균적으로 중소기업들은 DDoS 공격 탐지에만 약 9분이 소요된다는 점을 생각하면, 대응 속도가 매우 중요한 DDoS 공격 특성상 여전히 많은 부분이 아쉽다.

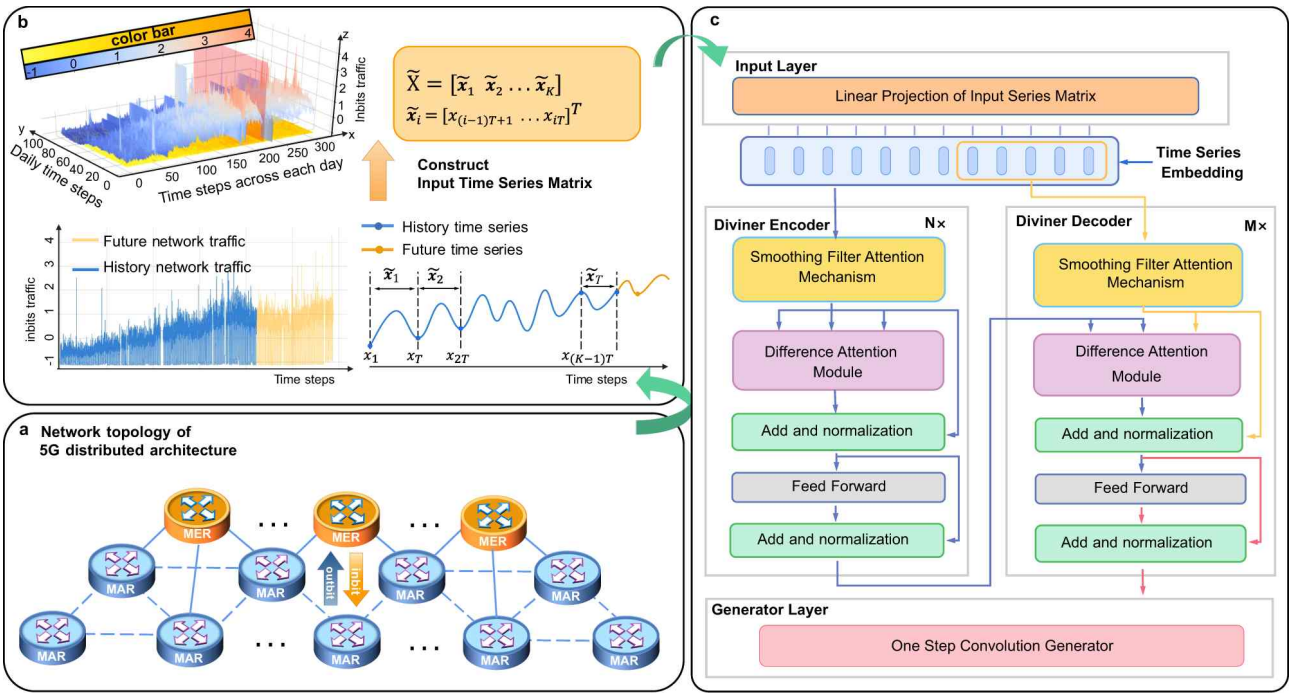
□ 아이디어

1.1 아이디어 요약

따라서 필자는 본 공모서를 통해 장기간의 예측에 적합하며, 시계열의 비정형성에 강한 모델인 Diviner 모델을 이용해 트래픽을 예측한 이후 미래의 DDoS 공격 가능 시점을 예상할 수 있는 방법을 제시하려고 한다.

1.2 Diviner 모델

Diviner 모델을 처음으로 소개하는 논문인 "Long term 5G network traffic forecasting via modeling non-stationarity with deep learning"에 따르면 Diviner 모델은 비정형성이 존재하는 5G 트래픽 데이터에서 트랜스포머 모델 구조에 Smoothing Filter Attention, Difference attention module, Feed Forward, 그리고 마지막에 One-step Convolution Generator를 추가해 트랜스포머 모델에 비정형성이 강화된 모델을 만들었다.



<Diviner 모델의 구조[3]>

특히 다른 트랜스포머 모델들과 다르게 Smoothing Filter Attention과 Difference attention 방법이 적용되는 것이 특징이다.

3) Yang, Y. Geng, S, Zhang, B, Zhang, J, Wang, Z, Zhang, Y, & Doermann, D. (2023). Long term 5G network traffic forecasting via modeling non-stationarity with deep learning. nature. Published: 06 June 2023.

1.2.1 Smoothing Filter Attention

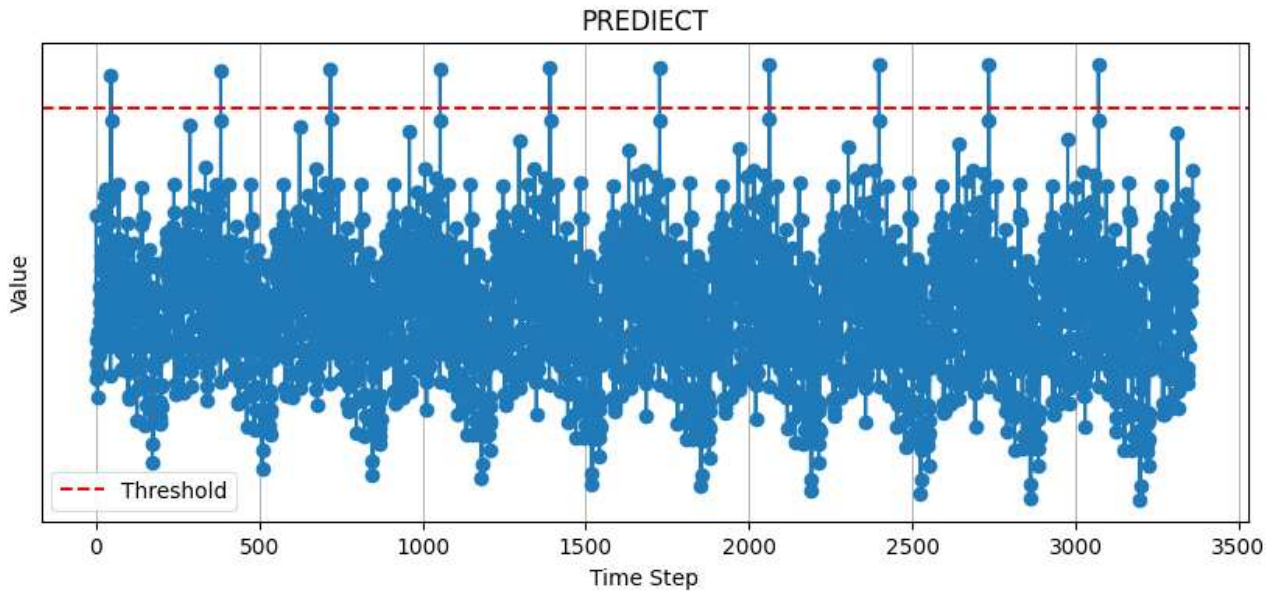
Diviner 모델이란 기존의 Self-Attention 방법을 사용해서 학습을 진행하는 트랜스포머 모델과 다르게 Nadaraya-Watson 회귀를 기반으로 하는 Smoothing Filter Attention 방법을 사용해서 데이터의 스케일을 조절한다. 따라서 다양한 스케일의 데이터에 적용할 수 있으며, 각 데이터에 가중치를 부여해 이상치의 영향과 데이터의 비정형성을 해소한다.

1.2.2 Difference-Attention-Module

데이터 간의 상관관계를 파악해서 각 타임스탬프 사이의 상관관계를 파악해서 학습할 수 있도록 유도한다.

1.3 Diviner 모델을 이용한 DDoS 탐지방법

① 우선 인코더에서 Smoothing Filter Attention를 통해 학습데이터에 가중치를 추가해서 비정형 데이터와 이상치를 제거한다.
② 인코더 층에서 difference attention 층을 거치고 각 타임스탬프의 차이를 학습한다.
③ 정규화, 모델 추가를 반복한다.
④ 인코더 출력값을 디코더로 보낸다. 그리고 디코더 역시 일부 데이터를 Smoothing Filter Attention로 보내서 전처리를 진행한다.
⑤ 인코더와 마찬가지로 difference attention, 정규화 등을 거친다.
⑥ cnn층에 입력후 예측값을 출력한다.
⑦ 모든 타임스탬프의 예측이 완료되면 특정 임계점 이상을 트래픽이 몰리는 구간으로 설정한다.



그 결과 트래픽이 몰리는 특정 구간대를 잘 예측하는 모습을 볼 수 있다.

1.4. 기존 연구와의 분석

기존의 순수 통계적 모델에 기반으로 한 방식과 RNN 모델을 기반으로 한 예측 모델과 다르게 Diviner 모델을 기반으로 한 트래픽 예측 방식은 장기간의 예측력을 매우 높였으며, 트랜스포머 모델과 다르게 Smoothing Filter Attention을 사용하는 등 비정형성에 대한 모델의 강건성 역시 높여 기존의 연구에 비해 예측 모델의 강건성과 성능 둘 다 개선한 방법이다.

□ 결론

1.1 기대 효과

1.1.1 DDoS 공격에 대해 사후 대응이 아닌 사전 대응

초당 대규모 트래픽을 통해 공격을 시도하는 DDoS 공격의 최고 대책은 빠른 대처다. 하지만 대부분의 국내 중소기업은 인력 부족 등 여러 가지 이유로 빠른 대응이 현실적으로 어렵다. 따라서 만일 사전에 DDoS 공격을 어느 정도 예상할 수 있다면 더 빠른 조기 대응이 가능하게 될 것이다.

1.1.2 KISA의 디도스 사이버 공격 대피소와 연계

DDoS 공격 이외에도 트래픽 플러딩 등 대량의 트래픽을 이용한 공격이 존재한다. 이때 이런 트래픽 예측 모델을 사용한다면 DDoS 이외의 다른 공격 기법에도 많은 도움을 받을 수 있다. 기존의 디도스 사이버 공격 대피소는 디도스 공격을 받은 기업이 KISA에서 대규모 트래픽을 우회하는 방법으로 많이 진행되고 있다. 따라서 KISA 측에서는 기업의 사후 보고에 따라 대응할 수밖에 없는데, 만일 사전에 DDoS 공격을 어느 정도 예상할 수 있다면 트래픽이 미리 몰리기 전에 기업에 해당 사실은 고지하고 미리 디도스 사이버 공격 대피소에 트래픽을 우회할 수 있도록 준비해 DDoS 공격에 대해서 더 빠르게 대응할 수 있을 것이다.

1.1.3 다양한 트래픽을 이용한 공격에 응용 가능

DDoS 공격 이외에도 트래픽 플러딩 등 대량의 트래픽을 이용한 공격이 존재한다. 이때 이런 트래픽 예측 모델을 사용한다면 DDoS 이외의 다른 공격 기법에도 많은 도움을 받을 수 있다.

1.2 향후 계획

1.2.1 MLOPS를 기반으로 한 REAL-TIME 탐지 및 예측에 대한 자동화

MLOps는 Machine Learning Operations의 약자로, 기계학습 모델의 개발과 운영을 통합하고 자동화하는 방법론으로 DevOps와 기계학습을 결합하여, 모델 개발에서 운영까지의 전체 수

명 주기를 관리하고, 모델의 신속한 배포와 지속적인 모니터링, 최적화를 가능하게 하는 방법이며, 최근에는 mlflow를 비롯한 여러 mlops 서비스를 구축할 수 있는 방법들이 늘어나고 있다.
따라서 mlops를 기반으로 한 통합 data pipeline을 만들어서 추후에 추가적인 데이터 수집과 신규 모델의 도입 과정을 간소화하여 시계열 예측을 통한 하나의 통합 자동 감시 체제를 구축해야 한다.

1.3 마무리

4)최근 NETSCOUT의 DDoS THREAT INTELLIGENCE REPORT에 따르면 대한민국은 2023년 상반기에만 384,613회의 DDoS 공격이 기록되었다. 그리고 대한민국은 트래픽을 이용한 공격의 빈도에서 미국, 브라질, 사우디아라비아에 이어 4위를 차지하며, 이러한 공격의 전체적인 비율은 4.2%를 차지하고 있다.
공격의 빈도와 수법은 점점 더 정교하고 교묘해지고 있으며, 최근에는 랜섬웨어와 연계된 랜섬도스가 등장하면서 위험도가 상당히 증가하고 있다. 그러나 국내 중소기업들은 보안 인력 부족 등의 이유로 사이버 보안에 매우 취약하며 디도스에 대한 대응능력이 떨어지므로, 이제는 이들의 디도스에 대한 실질적인 해결책이 필요한 시점이다.
따라서 본 필자는 이런 문제를 해결하기 위해 기존의 디도스 공격 후 대응하는 방법에서 사전에 트래픽 예측 후 공격 위험 시점부터 KISA의 디도스 사이버 공격 대피소 정책 및 여러 사이버 인적자원과 연계해 DDoS에 좀 더 빠르게 대응하는 방법을 제시하고 있다.
결론적으로, 사전 트래픽 예측을 통한 디도스 공격의 사전 대응은 국내 중소기업의 사이버 보안 인력 부족 문제를 해결하고, 디도스 공격으로부터 보다 효과적으로 대비할 수 있는 방안을 제시한다. 특히 기존 KISA의 디도스 사이버 공격 대피소 정책과 연계하여 정책의 효과를 지금보다 더 극대화하면서 사이버 인적, 물적 자원을 활용하면, DDoS 공격에 빠르게 대응하고 이에 따른 피해를 최소화할 수 있을 것이다. 이러한 접근 방식은 기술의 발전을 통해 중소기업의 사이버 보안을 강화하고, 국내 사이버 보안 생태계를 더욱 견고하게 만드는 데 기여할 것이다.

4) NETSCOUT Threat Intelligence Report - APAC: Korea. Retrieved from https://www.netscout.com/threatreport/apac/korea/#:~:text=,Attack%20Frequency%20384%2C613%20Attacs

[참고문헌]

[1] 보안뉴스, “북한 추정 사이버공격, “2004년부터 2021년까지 300배 이상 증가했다”, 2022-05-09
[2] kbs, “디도스 공격 탐지 시간, 대기업 3분·중소기업 9분”, 2021-07-06
[3] IEEE,“Traffic Flow Forecast Through Time Series Analysis Based on Deep Learning”, 2021
[4] 한국통계학회, “시계열 모형을 이용한 통신망 트래픽 예측 기법연구”, 2007
[5] nature. “Long term 5G network traffic forecasting via modeling non-stationarity with deep learning”. 2023
[6] IEEE, “Traffic Flow Forecast through Time Series Analysis Based on Deep Learning”.2020
[7] *Neural Information Processing Systems* “Attention Is All You Need”. 2017
[8] NETSCOUT. “Threat Intelligence Report - APAC: Korea.”.2023

※ 분량 : 10페이지 이내