LSTM기반 소스 측 DoS공격 탐지에서 특징벡터 영향 평가

염성웅, 뉘웬 지앙 즈엉, 뉘웬 반 퀴엣, 김경백
전남대학교 전자컴퓨터공학부

Feature vector impact assessment in LSTM-based source-side DoS attack detection

Yeom Sungwung, Giang-Truong Nguyen, Van-Quyet Nguyen, Kyungbaek Kim
Dept. Electronics and Computer Engineering, Chonnam National University
E-mail:quyetict@utehy.edu.vn,truongnguyengiang.bk@gmail.com,sinhngoc.nguyen@gmail.com,
jefron1100@gmail.com, kyungbaekkim@jnu.ac.kr

요 약

엣지 컴퓨팅의 발달에 따라 소스 측 DoS 공격 탐지를 위한 다양한 연구가 진행되고 있다. 최근LSTM을 활용하여 소스 측 네트워크 트래픽을 예측해 DoS공격을 탐지하는 기법이 제안되었다. 하지만, DoS 공격 트래픽의 변화가 미묘하다면 정상 트래픽과 섞여 잘못된 탐지 결과가 발생할 수 있다. 특히, 정상 트래픽을 DoS 공격으로 탐지하는 False positive rate가 높아진다. 이러한 오탐율은 LSTM 기반 트래픽 예측율과 상관관계가 있고 LSTM에 사용되는 입력벡터의 정보에 따라 그 성능이 달라질 수 있다. 본 논문에서는 LSTM의 입력 벡터가 소스 측 DoS탐지 기법에 미치는 영향을 분석한다. 입력 벡터로는 관측된 트래픽 양의 변화율, 해당 time window 인덱스 그리고 트래픽 변화 트랜드(Seasonality)를 사용한다. 특히, 트래픽 변화 트랜드를 3가지 또는 9가지 상태로 표현하고, 각 경우에 대한 Dos 탐지기법의 성능을 비교 분석한다. 실제 DNS 트래픽 기반의 실험을 수행하여, 3가지 상태에 비해 9가지 상태의 트래픽 변화 트랜드를 사용할 경우, LSTM 기반 DoS 공격 탐지 기법의 False Positive rate를 35% 이상 줄일 수 있음을 확인하였다.

1. 서 론

DoS 공격은 매우 쉽게 시작할 수 있고 치명적인 서비스 손실을 초래할 수 있으며, 공격자를 추적하기가 어렵다. 최근 DoS 공격에 대응하기 위해 소스 측에서 네트워크 트래픽 이상 감지 연구가 이루어지고 있다. 특히, LSTM (Long Short-Term Memory) 기반의 네트워크 트래픽 볼륨을 추정하여 공격을 탐지하는 기법[1][2]이 연구되었다.

소스 측 트래픽 볼륨기반 DoS공격 판별 기법은 공격 트래픽이 쉽게 정상 트래픽과 섞일 수 있다는 점을 감안하여, 보다 세밀한 공격탐지 임계값을 설정하고 주기적으로 임계값을 바꾸어야 한다. 이때, 공격 탐지 후 공격탐지 임계값을 갱신할 때, 공격트래픽과 정상트래픽을 분리해 사용해야 한다. 이를 위해 LSTM을 이용해 정상트래픽의 변화량을 추정하고, 이를 기반으로 공격이 탐지된 상황에서 유효한 수준의 정상트래픽을 추출해 공격탐지 임계값을 갱신할 수 있게 된다. 또한, 이러한 보다 세밀한 임계값 설정을 통해 공격탐지 기법의 False Positive를 줄일 수 있다.

이러한 LSTM기반 소스 측 트래픽 볼륨기반 DoS공격 판별기법은, LSTM의 정상트래픽 추정성능에 의해 그 성능이 영향을 받게 된다. 특히 LSTM 구조 뿐만 아니라 입력벡터의 종류와 형식에 따라서 성능에 차이가 생길 수 있다.

이 논문에서는 LSTM기반 소스 측 트래픽 볼륨기반 DoS공격 판별 기법에서, LSTM 학습에 이용되는 입력벡터의 변화가 판별기법에 미치는 영향을 분석하고 평가하였다. 기본적으로 LSTM의 입력벡터는 트래픽 별화율, 시간, 트래픽 트렌드(Seasonality)의 세 가지 도메인으로 구성되어있다. 여기서, 트래픽 트렌드의 경우, 상승(Increasing), 하강(Decreasing), 혼조(Fluctuating)의 세 가지 상태를 가질 수 있다. 또한, 트래픽 트랜드 세 가지 상태간의 변화를 고려하는 것도 가능하다. 즉, 상태 값을 사용할 경우 트래픽 트렌드는 3bit로 표현하고, 상태 간 변화 값을 사용할 경우 트래픽 트렌드는 9bit로 표현이 가능하다. 이러한, 서로 다른 입력벡터를 사용할 때, LSTM기반 공격탐지 기법의 공격탐지률(Detection Rate)와 공격오탐률(False Positive Rate)를 측정하여 각 입력벡터의 영향을 평가하였다.

2. LSTM 기반 트래픽 예측 및 DoS 공격 탐지

소스 측에 들어오는 네트워크 트래픽은 게이트웨이에서 캡처할 수 있다. 결과적으로 일정 시간 t_w로 동일한 기간으로 분할된 time window 내에서 네트워크 트래픽 볼륨을 관측할 수 있다. 이 논문에서는 t_w를 1분으로 설정했다. 우리는 z^{th} time window에서 관찰된 트래픽 량을 s_z

로 정의한다. Exponential smoothing 함수에 의해, z^{th} time window에서 예측된 트래픽 량은 $s_z = \alpha * s_{z-1} + (1-\alpha) * s_{z-1}$에 의해 계산되어진다. α는 Exponential smoothing 파라미터이다. 논문[7]에 따라, z^{th} time window에서 threshold 값 θ_z는 $\theta_{z-1} = (1+\delta) * s_z$에 의해 계산된다. 즉, False Positive rate을 줄이기 위해 θ_z는 Margin$\delta(0 < \delta < 1)$에 의해 Leverage된다. s_z가 θ_z보다 크면 z^{th} time window내 트래픽들을 공격으로 인지한다. 다음 time window θ_{z+1}에서 threshold 값을 계속 업데이트하기 위해 정상 트래픽 $s_{z_{predict}}$를 예측해야한다.

우리는 $s_{z_{predict}} = s_{z-1} * \Delta_z$를 계산하는데 사용될 z^{th} time window에서 트래픽 볼륨의 seasonality Δ_z를 고려한다. 논문 [8]에서 보듯이, Δ_z는 LSTM 신경회로망을 학습함으로써 계산될 수 있다. 즉, 이전 시계열 입력베터 $I_{i-n}, I_{i-n+1} \cdots I_{i-1}$ 를 LSTM 신경 회로망에 넣어 i번째 time window에 해당하는 트래픽 변화량인 ch_i (changing vector) ($ch_i = \frac{s_i}{s_{i-1}}$)를 예측하는 LSTM 모델을 학습한다. 이때, $I_t(i-n < t < i-1)$는 LSTM에서 사용되는 입력벡터로, 이는 트래픽 변화량(ch_t), time window 인덱스(t),트래픽 트렌드(trend state) 3개의 특징으로 구성된다. 이중 트래픽 트렌드의 경우, 그림1과 같이 현재 time window의 3가지 상태 (increasing, decreasing, fluctuating)를 3bit 스트림으로 나타낼 수 있다. 또한, 그림 1에서 보는 변화 에지와 같이 이전 time window에서 현재 time window로의 트렌드 상태변화를 표현하는 9bit 스트림을 트래픽 트렌드로 이용할 수 있다.

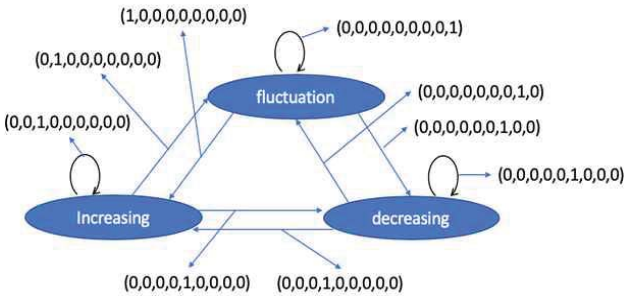

그림 1. State diagram of traffic trend

3. 실험 및 검증

서로다른 입력벡터가 LSTM기반 소스측 DoS공격탐지 기법에 미치는 영향을 평가하기 위해 DNS-STAT: Hedgehos[9]의 DNS 질의에 기반한 시뮬레이션을 수행하였다. 2018 년의 첫 30 일에 해당하는 DNS 질의 트래픽을 사용하여 LSTM을 학습한 후 다음 10일간의 DNS 질의에 DoS공격을 추가한 데이터 트래픽을 이용해 DoS공격 탐지 기법의 성능을 측정하였다. LSTM 네트워크 학습을 위해 Gradient descent optimization 알고리즘과 크기가 100인 배치를 사용하였고 1000번의 학습을 반복하였다. 또한, 기존의 다른 방법과의 평가를 위해 Static threshold method[4], OTAT 알고리즘[7], LSTM 기반 공격탐지 (3 state [2], 9 state)에 대한 실험을 수행하였다.

그림 2는 margin δ의 변화에 따른 각 탐지기법의 공격탐지율(Detection Rate)을 나타내고 있고, 그림 3은 margin δ의 변화에 따른 공격오탐율 (False Positive Rate)를 나타낸다. Static 기법의 경우 소스측 공격을 탐지하는 것이 힘든 것을 확인 할 수 있다. 반면 OTAT와 LSTM기반 기법은 적절한 Margin (<4%)을 가질 경우 높은 공격탐지율을 가진다. 하지만, OATA의 경우 50%이상의 공격오탐율일 가지는 것을 알 수 있다. LSTM기반 기법의 경우 OATA보다는 보다 낮은 공격오탐율을 가진다. 특히 9 state를 활용한 입력벡터를 사용하여 학습한 LSTM기반 공격 탐지 기법은 3 state를 활용한 입력벡터를 사용하는 경우에 비해 공격오탐율을 30%정도 줄일 수 있음을 확인하였다.

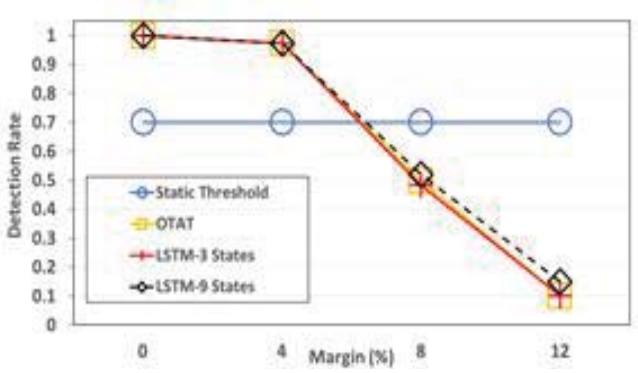

Figure 2. Detection rate with different margin

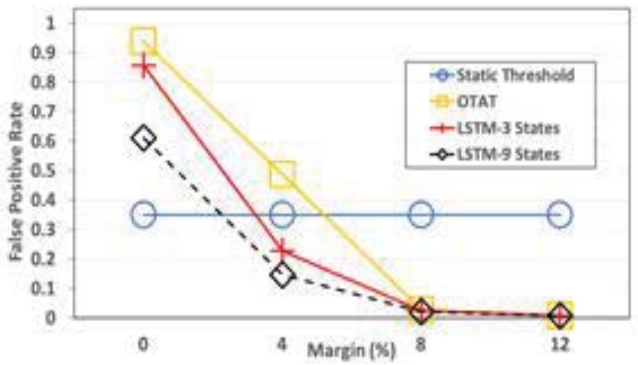

Figure 3. False positive rate with different margin

4. 결 론

본 논문에서는 LSTM의 입력 특징 벡터가 트래픽 변화율 예측 기반 소스 측 DoS 공격 탐지 기법에 미치는 영향을 분석하였다. LSTM의 입력 벡터로 관측 트래픽 변화의 9가지 상태를 이용할 경우 3가지 상태를 사용하는 경우에 비해 높은 Detection rate를 유지하면서 False Positive rate를 30% 이상 낮출 수 있다는 것을 확인하였다.

Acknowledgements

이 논문은 정보(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2017RIA2B4012559). 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터 지원사업의 연구결과로 수행되었음(IITP-2019-2016-0-00314)

참 고 문 헌

[1] Sinh-Ngoc Nguyen, Van-Quyet Nguyen, Giang-Truong Nguyen, JeongNyeo Kim and Kyungbaek Kim. “Source-Side Detection of DRDoS Attack Request with Traffic-Aware Adaptive Threshold.” IEICE Transactions on Information and Systems, Vol.E101-D,No.6,pp.1686-1690, JUNE 2018.

[2] Giang-Truong Nguyen , Van-Quyet Nguyen, Huu-Duy Nguyen, Kyungbaek Kim. “LSTM based Network Traffic Volume Prediction” 2018 KIPS Fall conference.

[3] Gandomi, Amir, and Murtaza Haider. “Beyond the hype: Big data concepts, methods, and analytics." International Journal of Information Management35.2 (2015): 137-144.

[4] Wang, Jie, et al. "The crawling and analysis of agricultural products big data based on Jsoup." Fuzzy Systems and Knowledge Discovery (FSKD), 2015 12th International Conference on. IEEE, 2015.

[5] Chen, Shuangxi, et al. "Analysis of plant breeding on hadoop and spark." Advances in Agriculture 2016 (2016).

[6] Hadoop, Apache. "Apache Hadoop". http://hadoop.apache.org (2017).

[7] Zaharia, Matei, et al. "Spark: Cluster Computing with Working Sets." HotCloud 10.10-10 (2010): 95.

[8] Van-Quyet, Nguyen, et al. “Design of a Platform for Collecting and Analyzing Agricultural Big Data.” JDCS vol. 18, no.1, pp. 149-158, 2017

[9] Agrawal, Rajeev, et al. "Challenges and opportunities with big data visualization." Proceedings of the 7th International Conference on Management of computational and collective intElligence in Digital EcoSystems. ACM, 2015.

[10] Liu, Zhicheng, et al. "imMens: Real time Visual Querying of Big Data." Computer Graphics Forum. Vol. 32. No. 3pt4. Blackwell Publishing Ltd, 2013.

[11] Sucharitha, V., et al. "Visualization of big data: its tools and challenges." International Journal of Applied Engineering Research9.18 (2014): 5277-5290.

[12] Wang, Lidong, et al. "Big data and visualization: methods, challenges and technology progress." Digital Technologies 1.1 (2015): 33-38.

[13] Dean, Jeffrey, and Sanjay Ghemawat. "MapReduce: simplified data processing on large clusters. " Communications of the ACM 51.1 (2008): 107-113.

[14] Thusoo, Ashish, et al. "Hive: a warehousing solution over a map-reduce framework." Proceedings of the VLDB Endowment 2.2 (2009): 1626-1629.

[15] Savasere, A., Omiecinski, E. R., & Navathe, S. B. (1995). “An efficient algorithm for mining association rules in large databases”. Georgia Institute of Technology.