Proceedings of International Conference on Educational Discoveries and Humanities
Hosted online from Plano, Texas, USA.
Date: 1st January, 2024
ISSN: 2835-3196 **Website:** econferenceseries.com

NETWORK INTRUSION DETECTION BASED ON MULTI-DOMAIN DATA AND ENSEMBLE-BIDIRECTIONAL LSTM

Korotkova Larisa Aleksandrovna
Senior Lecturer, Tashkent State Technical University
Department: radio devices and systems

Yuldasheva Diyora Ravshanovna
2nd Year Student

Abstract

Different types of network traffic can be treated as data originating from different domains with the same objectives of problem-solving. Previous work utilizing multi-domain machine learning has primarily assumed that data in different domains have the same distribution, which fails to effectively address the domain offset problem may not achieve excellent performance in every domain. To address these limitations, this study proposes an attention-based bidirectional long short-term memory (Bi-LSTM) model for detecting coordinated network attacks, such as malware detection, VPN encapsulation recognition, and Trojan horse classification. To begin, HTTP traffic is modeled as a series of natural language sequences, where each request follows strict structural standards and language logic. The Bi-LSTM model is designed within the framework of multi-domain machine learning technologies to recognize anomalies of network attacks from different domains. Experiments on real HTTP traffic data sets demonstrate that the proposed model has good performance in detecting abnormal network traffic and exhibits strong generalization ability, enabling it to effectively detect different network attacks simultaneously.

Introduction

The Ethernet protocol has been widely used in recent decades. One of the significant properties of Ethernet protocols is that they are partially open source and designed with security policy flaws , which means that network equipment is vulnerable to serious security threats such as viruses, Denial of Service (DoS) attacks, and port cracking access. As

software systems and applications become increasingly complex, more and more vulnerabilities have emerged, causing great harm to network security. Network intrusion detection is a means of network protection, which aims to analyze the network traffic, log data, and related information and discover abnormal traffic data from a large set of data streams. Once the network traffic is recognized as abnormal, it can be considered as an attack on the network so that related measures must be taken in advance to avoid catastrophic loss. Basically, existing network anomaly detection methods can be divided into two categories: one is based on feature distribution, and the other is based on content detection. However, these methods often lack the ability to distinguish between different types of attacks, leading to inaccurate detection of some anomalies. Recent studies have proposed using machine learning techniques to discover abnormal behavior from HTTP server logs and cluster HTTP session processes using a non-parametric hidden Markov model with explicit state duration. Additionally, some researchers have used unsupervised deep belief networks (DBNs) to extract low-level features and trained single-class support vector machines (SVMs) to perform anomaly detection and diagnosis from network traffic. These methods usually only involve the detection of a single type of traffic and cannot automatically extract and identify the key features of multiple types of traffic.

Related work

For the purpose of network intrusion detection, machine learning approaches such as cluster analysis, Bayesian networks, particle algorithms, and other shallow algorithms are commonly used. Most of the algorithms can learn enriched features of the data, but they are difficult to be used in practical scenarios due to different means of intrusion and heterogeneous distributions of the data. Network intrusion detection based on deep learning is independent of feature engineering and can automatically learn complex features from raw traffic data. Therefore, many scholars have applied neural networks to network intrusion detection tasks. Due to the improvement of the traffic classification accuracy,

network anomaly detection based on neural networks has become a hot research topic in academia. Representative examples with respect to these studies are follows. The authors in the literature first mapped network traffic features to strings and translated the network traffic classification problem to text classification in natural language processing. They used recurrent neural networks (RNN) to learn temporal features of network traffic and further used it for malicious network traffic detection. The authors in the literature proposed a malware traffic classification algorithm based on convolutional neural networks (CNN) for intrusion detection by mapping traffic features to generate grayscale pixel images. They processed network intrusion detection with network traffic image classification. The authors in the literature made a relevant summary of learning models, focusing on traffic data simplification, dimensionality reduction, and classification techniques. They proposed fully convolutional networks, which proved the effectiveness in analyzing the network traffic. In addition, the authors in the literature proposed an anomalous traffic detection method based on long-short-term memory (LSTM) with improved residual neural network optimization, which addressed the disadvantages such as overfitting and gradient disappearance in deep neural networks. As a result, the proposed model improved the accuracy of network anomalous traffic detection.

List of used literature

1. S. Zhao, Y. Fang, L. Qiu, Deep Learning-Based channel estimation with SRGAN in OFDM Systems.
2. G.E. Hinton, R.S. Zemel, Autoencoders, minimum description length, and Helmholtz free energy.
3. Y. Sui, Y. He, T. Cheng, Y. Huang, S. Ning, Broad echo state network for channel prediction in MIMO-OFDM systems.