Paper Summary
netFound: Foundation Model for Network Security

Sarthak | 2020CS10379

June 2024

Problem Statement

The paper addresses the challenge of constructing a generalized and transferable model for network security without the need of artificial feature engineering or large labeled traffic data

Motivation

- Existing network security methods require complex feature engineering and extensive data labeling, which hampers generalizability, thus necessitating a foundation model
- To effectively capture the hidden networking context, foundation models need to consider domain-specific attributes and constraints
- Networking packets are multi-modular and follow hierarchical structure, which differentiate them from other ML applications like NLP

Key Idea

To develop a transformer based network security foundation that handles the unique aspects of network packets :

- To handle the multi-modal nature of network data, input embedding method fuses information from packet fields at various granularities
- To capture the inherent hierarchy in network data, hierarchical transformer that enables parameter sharing across different granularity levels is proposed

Framework & Methodology

Data Pre-procesing

1. Data Extraction :

   - Packets within a flow are categorized into “bursts”
   - BURST is generated based on the principle of same direction and continuity
   - Then, the number of packets per burst and bursts per flow are standardized adopting the median value.

2. Featurization : For each packet in a burst, various network, transport, and application layer packet fields are extracted, transforming these raw fields into a fixed-size vector

3. Tokenization : We tokenize the extracted packet-level feature vector. 2-byte tokens are selected.

0.1 Token Embedding

This step converts a set of tokens at different granularity lev- els to discrete one-hot representation of each token into a continuous representation that is differentiable. Three types of embedding for each token: packet field, positional, and metadata are applied.

Pre-training

1. Hierarchical Transformers with skip connection

   - First layer Burst encoder - takes as input all the tokens in each burst and outputs a hidden representation for each token
   - Second layer Flow encoder - The hidden representation along with positional encoding is given as input in this layer
   - Skip connections - This innovative design is introduced in the Flow Encoder to understand the correlation between bursts

2. Masked BURST Model

   - each token in the input sequence is randomly masked with 15% probability.
   - As the chosen token, we replace it with [MASK] at 80% chance
   - ET-BERT is trained to predict tokens at the masked positions based on the context.

Fine-tuning- Adapting scenario specific encrypted traffic

1. A Multi Layer Perceptron model for each task is prepared with only 2 layers and attacked at the top of netFound.

Contributions

- Developed the hierarchial transformer based foundation model for network security which takes into account the multi- modular and hierarchical traits of network packets
- The idea of skip connections in transformers can be applied to problems requiring the understanding of correlation between various input layers.

Strengths

- netFound compares a11 existing methods and achieve the best results in network security applications
- netFound is comparatively robust against masked labels and label noises
- Comparatively immune to few-shot and unbalanced scenarios and hence generalizable and tranferable

Weaknesses & Limitations

- Learning packet-level and host-level representations for network traffics is missing in the model
- Since Netfound was tested in offline(static) setup, dynamic and continuous changes in traffic will bring variations to the sample scenario
- Similar to other transformer-based foundation models, netFound can be vulnerable to adversar- ial attacks