Realtime Robust Malicious Traffic Detection via Frequency Domain Analysis

Lyu Jiuyang, Dec 12, 2021.

A novel system realizes **realtime** and **robust** detection of malicious traffic in high throughput networks.

Introduction

Authors: Chuanpu Fu, Qi Li, Meng Shen, and Ke Xu. CCS 2021.

Motivation

ML based methods cannot detect real-time attacks due to inefficient traffic features extraction in high throughput networks.

Related Work

Table 1: Comparing the Existing Malicious Traffic Detection Methods

Category of Detection Systems		Feature Extraction Methods	Zero-Day Detection	High Accuracy	Robust Detection	Realtime Detection	High Throughput	Task Agnostic
Rule based		Preconfigured fix rules [6, 29, 35]	×	✓	×	✓	✓	×
ML based	Packet-level	Packet header fields [53]	✓	✓	×	✓	×	✓
		Context statistics [42]	✓	✓	×	✓	×	✓
		Payload statistics [68]	✓	✓	×	×	×	✓
	Flow-level	Flow-level statistics [5, 37, 77]	✓	×	×	×	✓	×
		Application usage statistics [4, 28, 49]	✓	✓	×[1]	×	×	×
		Frequency domain features, Whisper	✓	✓	✓	✓	✓	✓

[1] Bartos *et al.* [4] only considered evasion strategies for malicious Web traffic.

Contribution

- We present Whisper, a novel malicious traffic detection system by utilizing frequency domain analysis, which is the first system built upon machine learning achieving **realtime and robust detection in high throughput networks**.
- We perform **frequency domain feature analysis** to extract the sequential information of traffic, which lays the foundation for the detection accuracy, robustness, and high throughput of Whisper.
- We develop **automatic encoding vector selection** for Whisper to reduce manual efforts for parameter selection, which ensures the detection accuracy while avoiding manual parameter setting.

Methodology

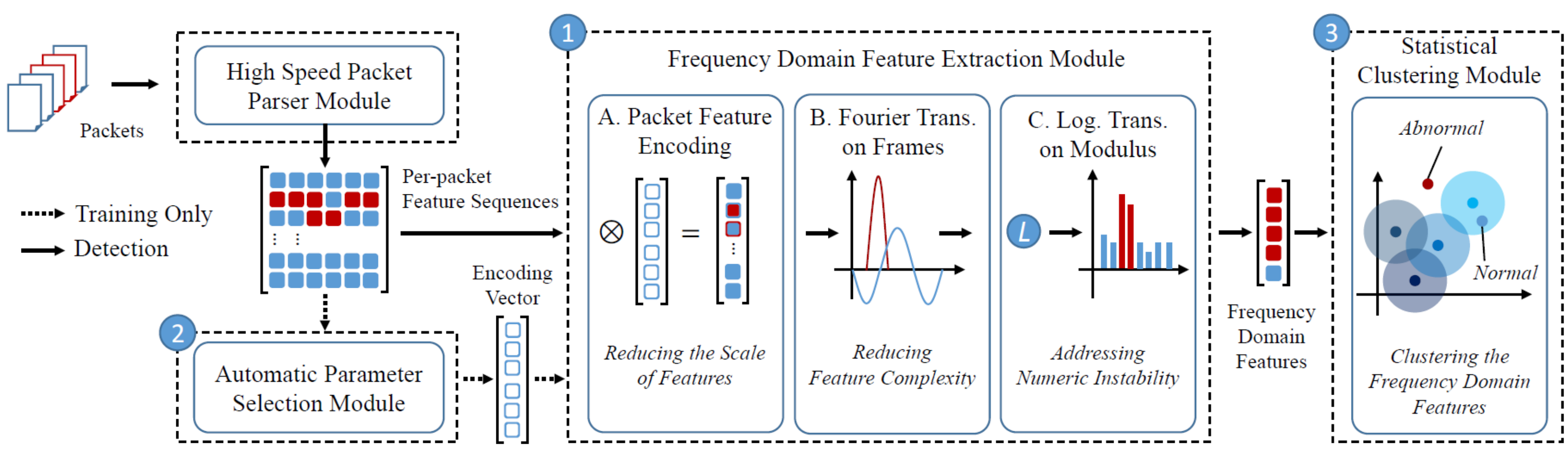


Figure 1: High-level design of Whisper.

1. Frequency Feature Extraction Module

Input: features of all packets.

Output: frequency domain features R

1. Per-packet features of all packets

$$\mathrm{S}=\left[s^{(1)},\ldots,s^{(i)},\ldots,s^{(M)}\right]=\begin{bmatrix} s_{11} & \cdots & s_{1M} \\ \vdots & \ddots & \vdots \\ s_{N1} & \cdots & s_{NM} \end{bmatrix}$$

2. Perform a linear transformation. The calculation of w_i will be described in next module.

$$v=Sw=\left[v_1,\ldots,v_i,\ldots,v_N\right]^{\mathrm{T}},\quad v_i=\sum_{k=1}^{M} s_{ik}w_k.$$

3. Segement the representation with a step length W_{seg}.
4. **Perform DFT on each frame**

$$F_i=\mathscr{F}\left(f_i\right)\quad\left(1\leq i\leq N_f\right)$$

$$F_{ik}=\sum_{n=1}^{W_{\mathrm{seg}}} f_{in}e^{-j\frac{2\pi(n-1)(k-1)}{W_{\mathrm{seg}}}}\quad\left(1\leq k\leq W_{\mathrm{seg}}\right)$$

5. Calculate the modulus of complex numbers
   - transform F_{ik} to a coordinate plane representation

$$F_{ik}=a_{ik}+jb_{ik}$$

$$\begin{cases} a_{ik}=\displaystyle\sum_{n=1}^{W_{\mathrm{seg}}} f_{in}\cos\frac{2\pi(n-1)(k-1)}{W_{\mathrm{seg}}} \\ b_{ik}=\displaystyle\sum_{n=1}^{W_{\mathrm{seg}}} -f_{in}\sin\frac{2\pi(n-1)(k-1)}{W_{\mathrm{seg}}}. \end{cases}$$

   - calculate the modules p_{ik} of F_{ik}

$$p_{ik}=a_{ik}^2+b_{ik}^2\quad\left(1\leq k\leq W_{\mathrm{seg}}\right)$$

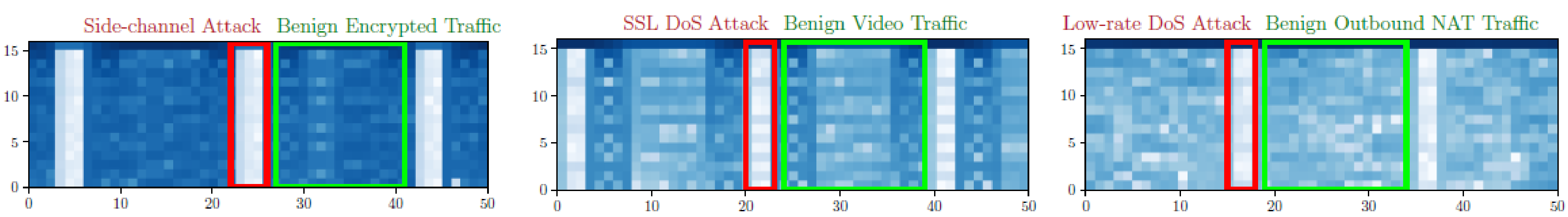
$$P_i=\left[p_{i1},\ldots,p_{iK_f}\right]^{\mathrm{T}}\quad\left(K_f=\left\lfloor\frac{W_{\mathrm{seg}}}{2}\right\rfloor+1\right)$$

$$F_{ik}=F_{i(W_{\mathrm{seg}}-k)}^{*}\Rightarrow p_{ik}=p_{i(W_{\mathrm{seg}}-k)}.$$

6. perform a logarithmic transformation on P_i, and use constant C to adjust the range of the frequency domain features

$$R_i=\frac{\ln\left(P_i+1\right)}{C}\quad\left(1\leq i\leq N_f\right)$$

$$\mathrm{R}_{K_f\times N_f}=\left[R_1,\ldots,R_i,\ldots,R_{N_f}\right]$$



(a) Benign TLS traffic and side-channel attack traffic (b) Benign UDP traffic and SSL DoS traffic (c) Outbound NAT traffic and LowRate TCP DoS traffic

Figure 2: We map the frequency domain features, which are extracted from the traffic with three types of typical attacks, to the RGB space, and observe that a small number of malicious packets incur significant changes in the frequency domain features.

2. Automatic Parameters Selection Module

Formulate the encoding vector selection problem as a constrained optimization problem.

$$\widetilde{w}=\arg\max\sum_{k=1}^{N} w_M n_{Mk}-w_1 n_{1k}-\sum_{i=2}^{M-1} 2w_i n_{ik}-w_{i-1}n_{(i-1)k}-w_{i+1}n_{(i+1)k}$$

subjects to:

$$\begin{cases} w_i & \in & [W_{\min}, W_{\max}] \\ \sum_{i=1}^{M} w_i n_{ik} & \leq & B \\ w_i n_{ik} & \leq & w_{i+1} n_{(i+1)k} \\ 2w_i n_{ik} & \leq & w_{i-1} n_{(i-1)k} + w_{i+1} n_{(i+1)k} \end{cases}$$

3. Statistical Clustering Module

1. Segment the frequency domain feature matrix R with a sampling window of length W_{win}
2. Perform the statistical clustering algorithm on the benign traffic and find its center

$$\hat{C}_i = \arg\min_{C_k} \|C_k - r_i\|_2 \quad (1 \leq i \leq N_t)$$

$$train\_loss = \frac{1}{N_t} \sum_{i=1}^{N_t} \left\| r_i - \hat{C}_i \right\|_2.$$

3. Detection

The traffic is malicious if $loss_i \geq \phi \times train\_loss$.

Theoretical analysis

A detailed theoretical analysis to prove Whisper's advantages.

Experiments

Dataset:

Table 4: Attack Dataset Configurations

Group	Label	Attack Description	Benign Traffic[1]	Benign Flow Rate	Malicious Flow Rate	Ratio of Malicious[2]
Traditional Attacks	SYN DoS	TCP SYN flooding Deny-of-Service attack.	2020.6.10	5.276 Gbps	23.04 Mbps	0.0858
	Fuzz Scan	Scanning for vulnerabilities in protocols.	2020.6.10	5.276 Gbps	27.92 Mbps	0.0089
	OS Scan	Scanning for active hosts with vulnerable operating systems.	2019.1.2	4.827 Gbps	0.960 Mbps	0.0045
	SSL DoS	SSL renegotiation messages flooding Deny-of-Service attack.	2020.1.1	7.666 Gbps	21.60 Mbps	0.0128
	SSDP DoS	SSDP flooding Deny-of-Service attack.	2020.1.1	7.666 Gbps	27.20 Mbps	0.0321
	UDP DoS	High-rate UDP traffic blocks bottleneck links.	2019.1.2	4.827 Gbps	2.422 Gbps	0.4712
Multi-stage TCP Attacks	IPID SC	Side-channel attack via IPID assignments, disclosed in 2020 [17].	2020.6.10	5.276 Gbps	0.138 Mbps	0.0007
	ACK SC	ACK rate limit side-channel attack, disclosed in 2016 [10].	2019.1.2	4.827 Gbps	1.728 Mbps	0.0091
	TLS Oracle	TLS padding oracle attack [67].	2020.1.1	7.666 Gbps	1.626 Mbps	0.0031
Stealthy TCP Attacks	LRDoS 0.2	UDP burst triggers TCP retransmissions (burst interval 0.2s).	2019.1.2	4.827 Gbps	0.115 Gbps	0.0228
	LRDoS 0.5	UDP burst triggers TCP retransmissions (burst interval 0.5s).	2019.1.2	4.827 Gbps	0.046 Gbps	0.0112
	LRDoS 1.0	UDP burst triggers TCP retransmissions (burst interval 1.0s).	2019.1.2	4.827 Gbps	0.023 Gbps	0.0055
	IPID Scan	Prerequisite scanning of the IPID side-channel attack [17].	2020.6.10	5.276 Gbps	0.214 Mbps	0.0010
	TLS Scan	TLS vulnerabilities scanning [38].	2020.6.10	5.276 Gbps	0.046 Gbps	0.0071

[1] The Benign Traffic column shows the identifier (date) of WIDE MAWI traffic datasets [69].
[2] The Ratio of Malicious column shows the packet number ratio of benign and malicious traffic.

Metrics: TPR，FPR(false-positive rates)，AUC，EER(equal error rates)

Results: achieve better AUC and stronger robustness than sota methods.

Other

The target of this article is to reduce the cost of machine learning methods, authors proposes many useful techniques, such as the use DFT to reduce dimensionality, and convert the parameter optimization problem into a constrained optimization problem. Also a strong theoretical analysis is displayed to prove Whisper's rationality