

加密网络流量智能检测方案

刘馥萱

2026/01/23

一、研究背景

- 随着 HTTPS / TLS 全面普及，网络流量中绝大多数已是加密流量，传统 DPI 和基于明文特征的检测不再可靠。
- 攻击者滥用加密协议隐藏 C&C 通信、恶意软件行为，检测难度增加。

由于加密流量无法解密所以导致无法直接使用Payload进行内容检测，此外传统ML误报率高以及对抗样本攻击会导致模型容易收到扰动误导

最新研究

- 最新研究提出利用图结构、无监督学习与对抗学习来提升未知/隐蔽流量检测能力
- 采用深度集成/多模型结构与表示学习提升检测准确率
- 未来趋势还包括自监督学习、弱监督学习降低对标注数据的依赖

Cai, S., Zhang, Y., Li, Y.

et al. DMSE: An efficient malicious traffic detection model based on deep multi-stacking ensemble learning. *Appl Intell* 55, 958 (2025). <https://doi.org/10.1007/s10489-025-06819-1>

二、研究目标

可在加密网络流量条件下进行恶意行为检测且具备对抗鲁棒性的智能系统

具体内容包括不依赖流量解密而是利用流量测信道特征或交互图，结合图神经网络提升泛化等。

三、研究内容

1. 特征表示创新

(1) 流交互图表示

传统流量表示主要是简单统计特征（字节数、包长、间隔、协议等），可引入流交互图表示（Flow Interaction Graph），利用流之间的关联关系构建图结构来提取行为模式，这种表示能更好反映恶意通信意图。

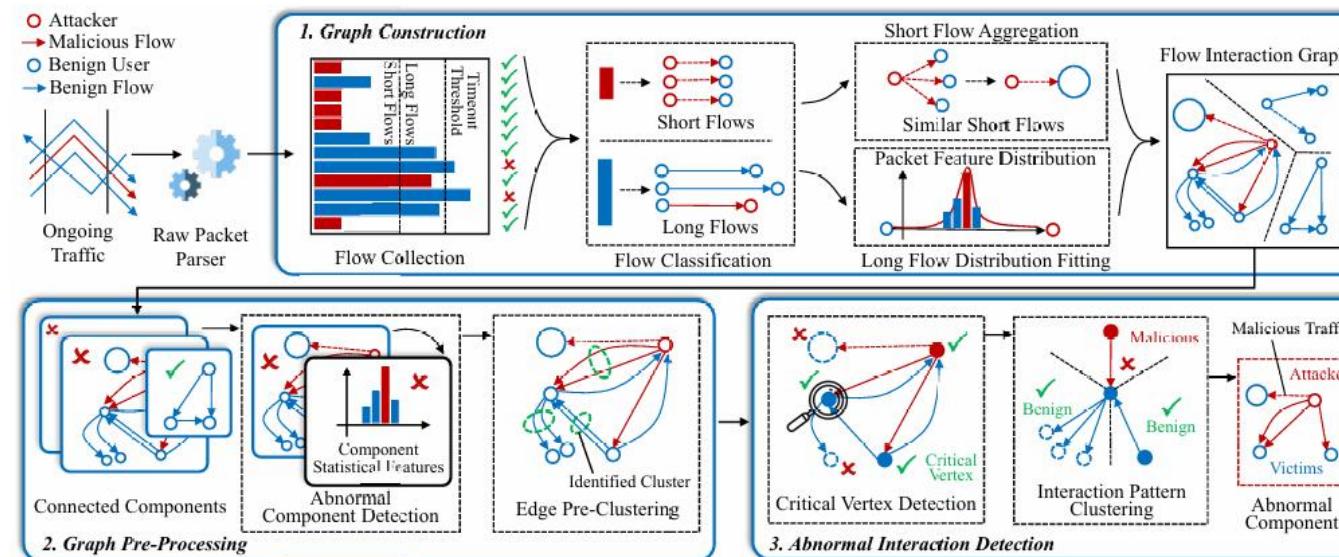


Fig. 1. The overview of HyperVision.

2. 自监督/对比学习模型

传统 Supervised Learning 依赖大量标注数据，且对未知样本泛化差，使用自监督或对比学习模型构建良好的流量表示空间，无须大量人工标注的前提下，自动学习网络流量的高层行为表示，从而有效提升模型对未知攻击与变种攻击的检测能力。

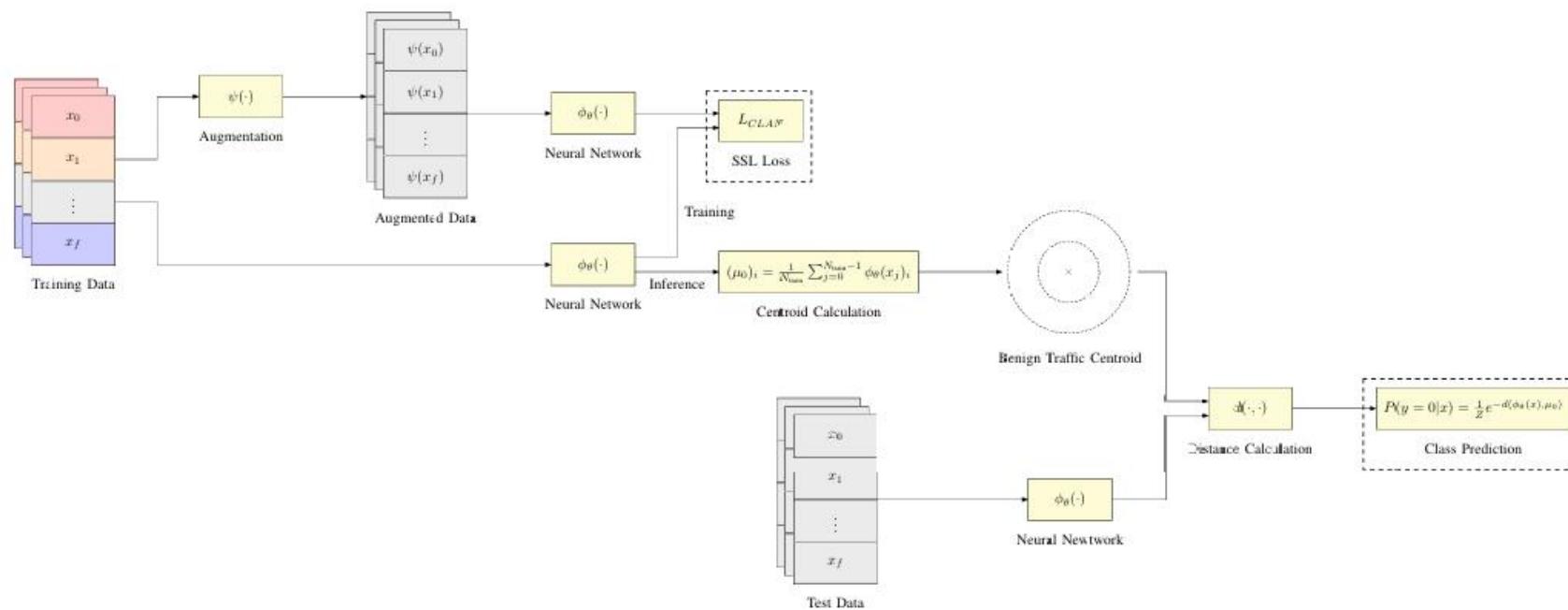
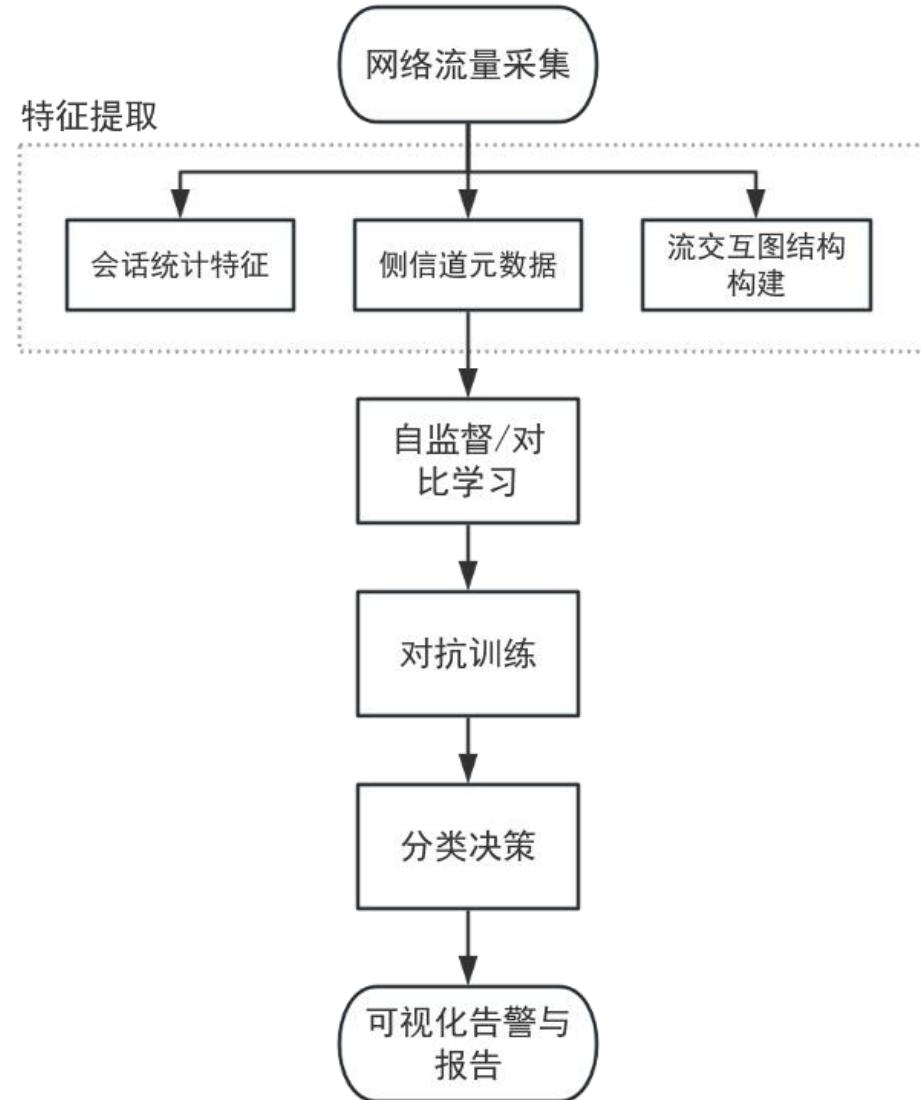


Fig. 1. Overview of the CLAN framework. A neural network is trained on both genuine benign and augmented network traffic to learn the distribution of benign traffic and map it to a single distribution in latent space. Evaluating the probability of a test sample belonging to this distribution can then be used to infer its label during inference.

3. 对抗鲁棒性

在真实对抗环境下，恶意流量会被特意扰动以逃避检测，可设计对抗示例生成 + 模型对抗训练以及评估模型在对抗样本下的鲁棒性，通过构造流量侧信道层面的对抗样本并进行联合训练，使检测模型在面对刻意规避行为时仍能保持稳定性能。

四、技术路线



五、数据集准备

- CIC-IDS 2017 / 2018
- UNSW-NB15 / ISCX Encrypted Traffic Dataset