# 恶意流量检测研究进展

关键字：恶意流量 识别 检测 研究进展

## 引言

恶意流量检测是当前的热点问题。随着移动互联网的普及和发展，网络流量的规模急遽上升，网民人数也在飞速增长中。随之而来的问题是，网络中加密流量和代理流量的比例越来越高。但恶意攻击利用加密技术隐蔽躲藏，Zscaler在2017年下半年的SSL威胁报告中表示，滥用SSL和TLS的网络钓鱼和恶意软件攻击事件显著增加。如何通过不解密的方法快速地进行网络流量的检测，并并更好的识别网络空间中的代理流量，保持较好的检测能力，成为一大重要课题。

原有基于IAIA体系为应用和协议进行了固定的端口号的分配，设计了基于端口号的流量分类方法。但现如今，当前的大部分应用都采用了动态端口分配这一方法。另外，一些网络服务，如隧道和匿名，隐藏了真实的端口号信息，后又提出了基于DPI（深度包检测）的流量分类方法，这种方法也无法适用于现如今tls加密下的场景，同时也大大增加了系统的存储开销，背离了网络安全保护的初衷。