DNS协议恶意行为检测系统

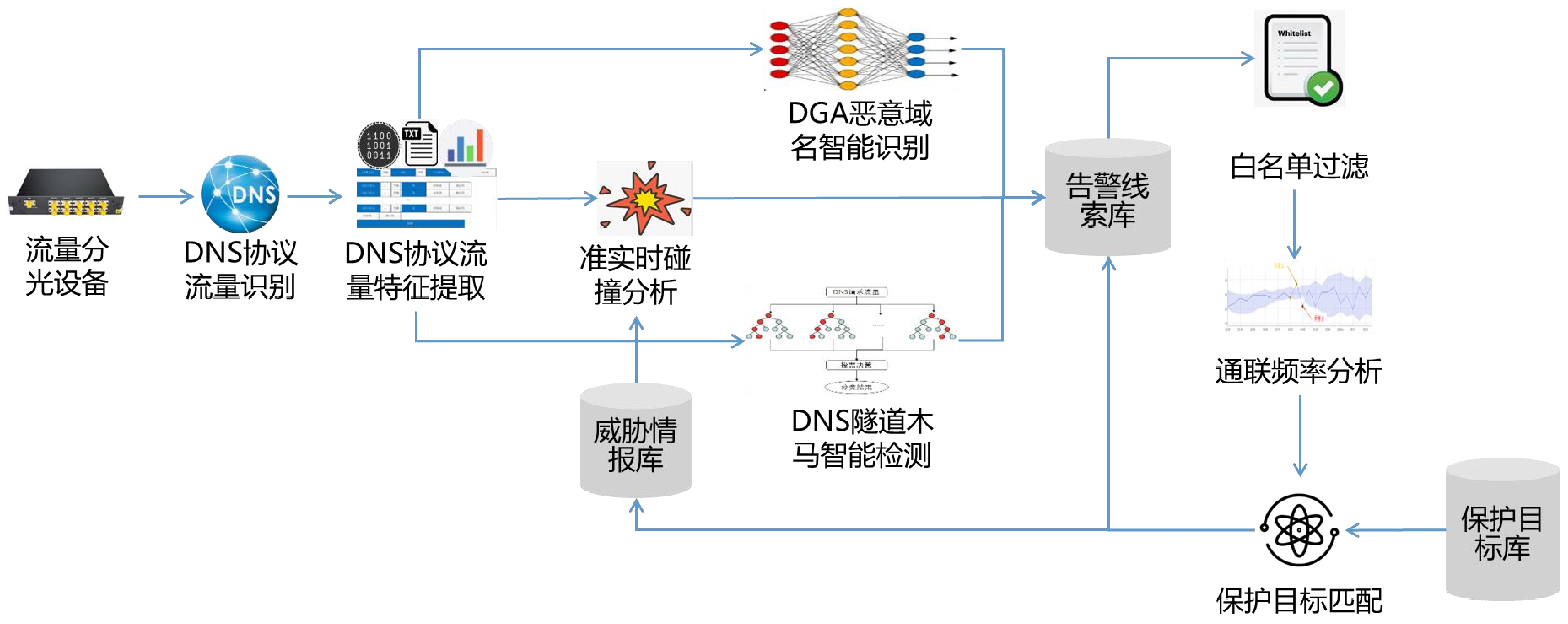
黄克振，张海霞，连一峰

联系方式：黄克振，15201067285，
kezhen@iscas.ac.cn

系统介绍

DNS是互联网地址翻译与路由中枢，实现网络域名与互联网数字地址之间的转换。然而，DNS协议在设计之初未充分考虑安全性，缺乏身份验证、协议设计缺陷等导致DNS欺骗、DNS隧道、命令与控制（C&C）通信等隐蔽性攻击高发，该类攻击极易绕过传统安全设备，难以检测发现与响应。针对这一问题，本系统在对相关攻击场景机制进行模拟和探究的基础上，引入融合注意力机制的卷积神经网络（CNN）、梯度提升树（GBDT）等智能算法，实现对DGA（域名生成算法）恶意域名、DNS隧道木马等未知威胁及其变异行为的有效识别，采用通信特征提取、通联规律分析、基线异常分类等手段，对检测结果进行智能降噪与关联，显著提升了DNS威胁行为检测的精准度。在某市城域网出口的实战应用表明，该系统可发现其他DNS协议检测设备难以发现的DNS加密回连、隐蔽数据传输、木马样本通信等可疑威胁，可为网络安全监管与保护提供有效技术手段支撑。

检测流程



系统界面