封面页

诚信承诺书

基于Zephyr的nRF52840双模键盘

摘 要

网络流量的预测及异常检测是实现下一代智能网络的关键技术之一。通过利用预测信息，网络运营商能够拥有足够长的时间来主动调整网络，从而积极应对网络需求的变化并保持高质量的传输性能，为用户提供平滑的用网服务。然而，网络流量及其模式是动态变化的，这为目前基于数据驱动的预测及异常检测算法带来了极大挑战。本文基于真实的网络流量数据，探索网络流量的特殊性质并用以指导设计基于高斯过程的在线流量预测与异常检测算法。具体而言，任务分成两部分：基于历史数据预测未来网络流量，检测预测流量是否存在异常。一方面，为了实现准确的网络流量预测，观察到网络流量的模式随时间动态演变，本文探索和利用不同时间和不同时间尺度的网络流量的特殊性质，并通过利用高斯混合模型动态地将一个主导模式和若干非主导模式编码至高斯过程的核函数中，以更好地应对网络流量特性的变化。另一方面，为了在流量特征随时间的推移而变化的背景下保持较高的流量分类准确性，本文首先利用KL（kullback-leibler）散度测量正常和异常流量之间的差异，将不断演变的流量统计量转化为静态特征。其次，为了对抗噪声和建模误差，根据网络流量的自相似性和周期性，设计了合适的特征向量。最后，采用稀疏表示技术降低训练数据收集的成本，以实现具有强鲁棒性的在线分类算法。进一步，本文通过基于GEANT数据集的仿真，并和若干基准算法比较，证实了提出的网络流量预测和异常检测算法的精确性。相关成果发表在IEEE Wireless Communications and Networking Conference 2023上（IEEE无线通信和网络会议，通信领域三大国际旗舰会议之一）。

关键词：网络流量；预测；异常检测；高斯过程；稀疏表示

English Abstract

Abstract

The forecast and anomaly detection of network traffic is a key enabler of smart management in next-generation networks, as sufficient amount of time can be provided for the proactive manipulation of network resources to maintain high quality transmission. Nevertheless, the evolving characteristic of network traffic challenges the current learning-based and data-driven algorithms on both prediction accuracy and anomaly detection accuracy. In this work, we explore special properties of network traffic, which are further encoded into the Gaussian Process (GP)-based online learning framework, so as to better comprehend, predict and detect future network traffic from a Bayesian perspective. Specifically, we proceed by two steps, 1). Observing network traffic is evolving, to explore and exploit the dynamic traffic patterns at different times and timescales, we try to approximate the optimal kernel function of GP by utilizing a mixture of Gaussian to encode the dominant and several nondominant patterns. 2). To combat noise and modeling error, we formulate a feature vector based on Kullback-Leibler (KL) divergence to measure the difference between normal and abnormal traffic, based on which SR is adopted to perform robust binary classification. Finally, we demonstrate the superiority of the proposed framework in terms of prediction and detection accuracy through simulation. We have presented a part of the content of this thesis at IEEE Wireless Communications and Networking Conference 2023, which is a flagship international conference of the communication society of IEEE.

**Key words:** Network traffic; Prediction; Anomaly detection; Gaussian process; Sparse representation

目录

[摘 要 2](#_Toc174913248)

[Abstract 3](#_Toc174913249)

第1章 绪论

1.1课题研究背景及意义

本项目采用挪威Nordic Semiconductor公司所设计的nRF52840 SoC，nRF52840基于带有浮点单元的32位Arm® Cortex™-M4 CPU，主频为64 MHz，有1MB的闪存和256KB的RAM。内置Arm TrustZone® CryptoCell密码算法单元，可独立于CPU高效执行密码算法任务。它支持多种无线协议，包括Bluetooth 5、Thread、Zigbee、ANT和2.4GHz。它还具有多种外设，包括ADC、PWM、SPI、I2C、UART、USB和GPIO等。通过精密的片上自适应电源管理系统，实现了极低的功耗。

本项目所设计的键盘在硬件方面：利用黑莓Q10手机的键盘作为按键矩阵，使用nRF52840作为处理核心，任天堂Switch Joy Con摇杆作为鼠标输入，附有若干微动开关作为鼠标按键。软件方面：运行以基于 Zephyr™ Project 实时操作系统 （RTOS） 构建的开源 （MIT） ZMK 固件，实时检测用户输入，经过处理后通过蓝牙或USB发送到连接的主机设备。

第2章 系统方案的总体设计

2.1 总体方案设计

本项目的控制系统选用