Toward an Explainable and Self-Adaptive SDN Framework for IoT Traffic Management

Muhammad Zain Uddin
Institute of Business Administration Karachi
Karachi, Pakistan
zuddin@iba.edu.pk

Syed Muhammad Faisal Iradat
Institute of Business Administration Karachi
Karachi, Pakistan
firadat@iba.edu.pk

Abstract

The exponential growth of the Internet of Things (IoT) device in era of smart life has introduced a wide range of devices that rigorously generate various and often unpredictable traffic. Managing this type of data flow in a network reliably and security has become increasingly difficult which lead us to the requirement of an adaptable network. Software Defined Networking (SDN), with its centralized control and programmable architecture, presents a solution for addressing these challenges in real time but still it require predefine rule to combat these challenges of upcoming traffic. In this paper, we propose a dynamic SDN-based framework that integrates machine learning methods for device type classification and prediction of their traffic patterns. Instead of using one model for all instances, we train specific classification and prediction models for every category of device. For enhanced transparency, we also add SHAP values to clarify the effect of varying features on each model's output. Our tests demonstrate that the classification model, developed based on XGBoost, achieves up to 98% accuracy on over 20 devices. For forecasting, our chunk-based strategy achieves a root mean squared error of minimum 0.05. These results highlight the potential of our approach to support anomaly detection, enable proactive bandwidth management, and build trust in model-driven decisions. To the best of our knowledge and research, this is the unique framework to integrate adaptive learning, forecast driven control, and explainability within an SDN setting for dynamic IoT environments.

CCS Concepts

• **Computing methodologies** → **Machine learning approaches**; • **Security and privacy** → **Network security**; • **Networks** → **Software defined networking**.

Keywords

Internet of Things (IoT), Explainable AI (X-AI), Machine Learning, Network Security, Device Classification

1 Introduction

A The rapid expansion of the Internet of Things (IoT) has resulted in highly heterogeneous networks where devices are highly dissimilar in purpose and behavior. Such networks generate bursty, unpredictable, and sometimes encrypted traffic that makes them difficult to manage and secure effectively [1]. Conventional SDN architectures offer centralized control, but are susceptible to be overwhelmed by workload bursts and scaling up to millions of devices[2]. IoT networks are being used more frequently in security-critical domains such as as healthcare and industrial automation. In these environments, unexpected traffic spikes or device misbehavior can compromise performance or introduce vulnerabilities. Predictive models can predict such changes ahead of time, enabling the SDN controller to dynamically redirect or throttle traffic in anticipation before something goes wrong. This proactive insight is the backbone of our suggested architecture. In order to enable this developing environment, we propose a framework that combines three elements:

- Accurate device identification using supervised ML techniques.
- Short-term traffic forecasting at the per-device level
- Model interpretability using SHAP-based explanation tools.

This architecture enables more proactive traffic handling while giving network operators the ability to verify and trust model behavior. Also, this idea at the initial level is also proposed in a conference without explainable adoption [4]

2 Research Aim

As this is a proposed Ph.D. idea, our work focuses on the following goals:

- Differentiate IoT device types using minimal yet informative traffic features.
- Anticipate device-level packet patterns using time-aware models.
- Provide transparent reasoning behind classification and prediction.
- Allow the system to adapt to changing traffic patterns without full retraining.

3 Approach

We utilize a labeled dataset containing packet-level traffic data from more than 18 IoT devices [3], each exhibiting different usage behaviors. Feature engineering focuses on size, port activity, and timing characteristics. Models tested include random forest, XGBoost, KNN, and neural networks. While our approach employs widely-used algorithms such as XGBoost and LSTM, the novelty lies in their integration into a unified and interpretable SDN-compatible framework. Specifically, we design (1) modular per-device predictors that scale independently, (2) chunk-based time series models that allow rapid adaptation to local behavior changes, and (3) SHAP-based interpretability to ensure decisions are explainable per device. This layered design allows precise, scalable, and auditable traffic control. To capture temporal trends, we employ chunk-based time series forecasting. This approach divides traffic into short segments that overlap, making it easier to adjust the models over time. We also introduce lagged features (e.g., prior packet sizes) to improve prediction quality. To make the models interpretable, we apply SHAP, a method that reveals the relative contribution of each input feature to a model's output. This step helps users understand why the system makes certain predictions and supports decision audits.

4 Summary of Results

Our experiments show that XGBoost yields the best classification results, achieving 98% accuracy across multiple device types. Time series predictions using the same model (with segmentation and lag features) produce low average error rates (RMSE <0.05-0.09). Feature explanations vary by device, but consistently highlight port and packet size attributes as influential. To validate the benefit of per-device models, we conducted a comparison against a unified model trained across all device traffic. The unified predictor achieved RMSE of 0.09, while per-device models achieved 0.05. The higher error in the unified model was due to overlapping patterns and conflicting traffic dynamics among devices, confirming the importance of modular predictors.

Table 1: Results summary

Task	Best Model	Score
Device Detection	XGBoost	98% accuracy
Forecasting	Chunked XGBoost	RMSE: 0.05–0.09
Explainability	SHAP	Clear, per-device attribution

The model's performance remained robust when tested with synthetic traffic variations. SHAP visualizations confirmed the system's ability to adapt to each device's unique behavior.

5 Contributions

This study introduces a modular framework for SDN-based IoT management that is both predictive and interpretable. Rather than relying on one-size-fits-all models, our system maintains separate predictors for each device type and updates them incrementally as traffic changes. This leads to reduced training cost, better accuracy, and enhanced operational transparency.

6 Future work

Our future work involves deploying the system in a simulated SDN environment to enforce traffic rules based on forecasts. We also plan to extend the model to handle encrypted traffic and introduce support for online learning to reduce latency between updates. Long-term, this research aims to inform the design of trustworthy and efficient networking systems for next-generation IoT deployments.

References

[1] Rajesh Kalakoti, Hayretdin Bahsi, and Sven Nõmm. [n. d.]. Explainable Federated Learning for Botnet Detection in IoT Networks. In *2024 IEEE International Conference on Cyber Security and Resilience (CSR)* (2024-09). 01–08. https://doi.org/10.1109/CSR61664.2024.10679348

[2] Baydaa Hashim Mohammed, Afifuddin Husairi, Hasimi Sallehudin, Fadele Ayotunde Alaba, and Nurhizam Safie. [n. d.]. A Conceptual Framework for Securing IoT-BIM. In *2022 Applied Informatics International Conference (AiIC)* (2022-05). 68–71. https://doi.org/10.1109/AiIC54368.2022.9914592

[3] Arunan Sivanathan, Hassan Habibi Gharakheili, Franco Loi, Adam Radford, Chamith Wijenayake, Arun Vishwanath, and Vijay Sivaraman. [n. d.]. Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics. 18, 8 ([n. d.]), 1745–1759. https://doi.org/10.1109/TMC.2018.2866249

[4] Muhammad Zain Uddin and Syed Muhammad Faisal Iradat. [n. d.]. IoT Pro-Active SDN: A Smart Predictive-Based Approach for IoT Devices in SDN. In *11th International Conference on Wireless Networks and Mobile Communications, WINCOM 2024, Leeds, United Kingdom, July 23-25, 2024* (2024), Syed Ali Raza Zaidi, Khalil Ibrahimi, Mohamed El-Kamili, and Abdellatif Kobbane (Eds.). IEEE, 1–6. https://doi.org/10.1109/WINCOM62286.2024.10657820