BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2025
http://excel.fit.vutbr.cz

Monitoring of Bluetooth Low Energy Devices

Matej Olexa*

Abstract

Bluetooth Low Energy (BLE) is widely used in IoT devices, creating security risks due to infrequent updates and monitoring challenges. This work presents an improved method for passive BLE connection detection. Our system (illustrated on the poster, Figure 1) uses a monitoring probe made out of three ESP32s to capture advertising packets from BLE devices, sending data to a Raspberry Pi 3B+ for analysis. We detect connections by analyzing the timing gaps between these packets [1]; significant pauses often indicate an active connection (example pattern shown in Figure 2 on the poster).
Building on our previous work [2], we employ a multi-input Multilayer Perceptron (MLP). Unlike prior models using single inputs [3], our MLP processes sequences of time deltas, leveraging temporal context to significantly improve generalization across diverse device behaviors.
This enhanced machine learning approach provides more accurate and robust connection detection, offering a practical, low-cost solution for security monitoring in environments with varied IoT devices.

*xolexa03@stud.fit.vutbr.cz, *Faculty of Information Technology, Brno University of Technology*

1. Introduction

Bluetooth Low Energy (BLE)[4] is now common in IoT devices for homes and offices. This creates security risks since many devices have vulnerabilities or receive few updates. Independent monitoring is important to detect misuse that might bypass device logs [2]. However, monitoring BLE is challenging due to its complex communication patterns and the high cost of specialized equipment, making it inaccessible for most users.

This work focuses on improving BLE connection detection using the pipeline illustrated in Figure 1 on our poster. The core components involve a 3 ESP32-based multi-sniffer probe for data capture and machine learning analysis performed on a Raspberry Pi. We collected a dataset of advertising packets from various devices in different environments, which was a focus during project practice – I contributed to [2], which this thesis builds upon. We then developed a machine learning model to analyze the timing of these packets, specifically the time gaps between them, to infer connection states. Our approach uses a multi-input Multilayer Perceptron (MLP) that processes sequences of advertising time deltas, allowing it to capture temporal context and improve generalization across different device behaviors.

2. Monitoring Methodology

Our approach monitors BLE connections by observing advertising packets. When a BLE device isn't connected, it regularly broadcasts advertising packets on channels 37, 38, and 39. When connected, these broadcasts typically pause or change pattern (an example pattern showing a connection pause is depicted in Figure 2 on the poster). By measuring the time between packets from a specific device, we can detect connections – a long pause often indicates an active connection[1].

We collected data from multiple devices using a monitoring probe which consists of three ESP32 microcontrollers, each monitoring one advertising channel. This setup ensures reliable packet capture. The ESP32s send captured data (device addresses and timestamps) to a Raspberry Pi for processing. The dataset [2] includes recordings from various IoT devices like smart locks, sensors, and lights, listed in Table 1.

For our analysis, we: 1. Filter packets to focus on a specific target device 2. Calculate time differences between consecutive packets from that device 3. Apply sampling techniques during model training to handle the imbalanced nature of the data (devices are disconnected most of the time)

Table 1. Devices contained in the dataset

Device class	Device
Lock	**Bentech** FP3
	Danalock V3-BTZE
	igloohome Padlock Lite
	Nuki Smart Lock 3.0
Lighting	**Philips** Hue **white**
	Revogi Bluetooth LED bulb
Actuator	**Philips** Hue Smart **plug**
Sensor	**Mi** Temp & Hum Monitor 2
	BeeWi Motion Sensor

3. Detection Method (MLP and CNN)

While the principle of using advertising gaps is established, simple statistical methods applied previously often resulted in high false positive rates. Earlier machine learning models also showed promise but struggled to generalize well across diverse devices, potentially due to using limited input context (e.g., only 1 packet per input) [3]. A model trained on one device type might not perform well on another with a different advertising interval or pattern.

To overcome this generalization challenge, we explored several neural network architectures, focusing primarily on Multilayer Perceptrons (MLPs), a type of feedforward neural network. Additionally, we investigated the potential of 1D Convolutional Neural Networks (CNNs) [5] for capturing patterns in the time delta sequences. For the MLP approach, we specifically investigated the benefit of providing temporal context to the model by comparing two main architectural ideas:

1. **Single-Input MLP:** A baseline model that classifies the connection state based on only the *current* 'Advertising Delta' value (after scaling).
2. **Multi-Input MLP:** Our proposed enhancement, which takes a *sequence* of the last N consecutive 'Advertising Delta' values as input. **We experimented with different sequence lengths (N) to determine the optimal amount of historical context.**

Our hypothesis is that by seeing a sequence of recent time gaps, the multi-input MLP can learn the device's 'normal' advertising rhythm and better distinguish a truly anomalous gap (indicating a connection) from mere fluctuations or the naturally long interval of a slow-advertising device. This ability to understand context, potentially influenced by the sequence length N, is key to improving generalization.

These models were implemented using the PyTorch Lightning framework for efficient training and evaluation. The output is a binary classification: 'connected' or 'not connected'. Standard metrics like F1-score, precision, and recall are used to evaluate performance, with a strong focus on consistent performance across different device classes and input configurations.

4. Conclusions

This work demonstrated an improved approach for passively detecting Bluetooth Low Energy connections using machine learning. Our key finding is that employing a multi-input MLP, which analyzes sequences of advertising time deltas, significantly enhances detection accuracy and generalization across diverse IoT devices compared to models using only single time-gap inputs [2]. By incorporating temporal context, the model better distinguishes between normal advertising patterns and connection-indicating pauses, leading to a more robust and practical monitoring solution. This method offers a viable low-cost alternative to expensive hardware analyzers, suitable for security monitoring in typical home and office environments.

Future work may explore sequence-aware models (e.g., LSTMs, GRUs), optimal sequence lengths, broader device testing, real-time optimization on Raspberry Pi, and integration with security frameworks.

Acknowledgements

I would like to thank my supervisor Mgr. Kamil Malinka, Ph.D., for his guidance and support throughout this project. I also want to thank Ing. Ondřej Hujňák, Ph.D., for his supervision during the project practice, which this thesis builds upon.

References

[1] Ondřej Hujňák, Kamil Malinka, and Petr Hanáček. Indirect bluetooth low energy connection detection. In *2023 International Conference on Information Networking (ICOIN)*, pages 328–333, 2023.

[2] Ondřej Hujňák, Kamil Malinka, Matej Olexa, and Petr Hanáček. Parallel ble advertising monitoring. Unpublished manuscript, 2024.

[3] Ondřej Hujňák, Patrik Holop, Kamil Malinka, Jakub Res, and Petr Hanáček. Machine learning supported bluetooth low energy connection monitoring. Unpublished manuscript, 2024.

[4] Bluetooth SIG. *Bluetooth Core Specification Version 6.0*, Dec 2023. Placeholder - Check official citation format for Bluetooth specifications.

[5] Ragav Venkatesan and Baoxin Li. *Convolutional Neural Networks in Visual Computing: A Concise Guide*. CRC Press, 10 2017.