Master's Thesis

Evaluation of Transport-Layer Protocols for BLE Communication in Industrial information

Abstract

In the rapidly expanding Internet of Things (IoT) ecosystem, Bluetooth Low Energy (BLE) has emerged as a dominant technology for short-range communication, particularly in edge computing scenarios where resource-constrained devices communicate with local gateways. BLE is especially prevalent in both consumer-grade IoT applications and Industrial IoT (IIoT) environments, where it facilitates device connectivity for monitoring, automation, and control systems.

BLE operates in two primary modes: 1/ advertising (broadcasting packets without a connection) and 2/ connected mode (which establishes a persistent link for data exchange). While advertising mode is relatively simple and robust—capable of functioning reliably even under poor signal conditions (low RSSI)—the connected mode, often used for bi-directional and secure communication, introduces several technical challenges. These include maintaining a stable link with minimal latency, ensuring robust performance in the presence of wireless interference, and optimizing energy consumption on battery-powered devices.

In practice, the connected mode is commonly used with TCP over TLS 1.3, a protocol stack that delivers strong security and reliable transmission. However, this conventional approach introduces significant protocol overhead and computational burden, which may be suboptimal for BLE's low-bandwidth, energy-sensitive, and intermittently connected operational contexts. These inefficiencies are especially pronounced in noisy environments with high packet loss or delay, which are common in industrial settings with dense wireless deployments.

Given these limitations, there is a growing need to systematically assess alternative transport layer protocols, such as QUIC, which promises reduced connection setup time, built-in encryption, and better handling of unreliable networks. This research aims to evaluate and compare communication stacks for BLE-based IoT applications—focusing on performance metrics like latency, reliability, energy efficiency, and security—through a combination of simulation and empirical testing in realistic scenarios.

This thesis will be conducted in collaboration with Dr. Maryam Eftekhari at Hilti Entwicklungsgesellschaft mbH, and will contribute to the broader understanding of protocol stack optimization for constrained wireless communication in IoT and IIoT systems.

Content

We identified the following research questions: * What are the performance limitations of using TCP over TLS 1.3 in BLE-connected mode for IoT applications? * Which alternative transport-layer protocols offer better performance under BLE constraints? * How do these protocols compare in terms of latency, throughput, packet loss, power consumption, and reliability? * How do different BLE antenna characteristics and RSSI levels affect protocol performance? * Which protocol stack provides the best trade-off between security, performance, and energy efficiency in industrial IoT environments?

To comprehensively assess the suitability of various transport layer protocols for BLE-connected mode in industrial IoT (IIoT) environments, this thesis employs a hybrid evaluation methodology that combines both network simulations and, where feasible, real-world hardware experiments. This dual approach ensures both scalability in testing and practical validation.

For simulations we will rely on the ns-3 network simulator, which offers fine-grained control over wireless network parameters and supports BLE protocol modeling [1]. Moreover, interference from non-BLE devices like WiFi can be easily simulated. As simulation setup we consider a network to model BLE connections under varying conditions such as RSSI, packet error rate, and device movement. The identified performance metrics are: latency, packet loss, throughput, handshake time, and power consumption for each protocol in various scenarios. For realistic channel simulation it is also possible to connect ns3 to the Sionna raytracing simulator [2].

If feasible, we aim to validate simulation results using physical BLE devices communicating with a gateway.

Contact:
Anatolij Zubow: <zubow@ccs-labs.org>

Requirements

Basic knowledge of wireless communication (Bluetooth LE), interest in IoT and practical skills (C++, Python, Matlab).

[1] BLE module for ns3, https://gitlab.com/Stijng/ns3-ble-module

[2] Zubow, Anatolij, et al. "Ns3 meets Sionna: Using realistic channels in network simulation." arXiv preprint arXiv:2412.20524 (2024).