Transport layer security for Internet of Things devices to cloud server communication

A Home Energy Management System (HEMS) can minimize domestic electricity cost by using price data to control applicances. These communications can be modeled with a publish/subscribe architecture, which is implemented by the Message Queuing Telemetry Transport protocol (MQTT), an application layer protocol for the Internet of Things (IoT). In contrast, common protocols are typically request/response-based. The communication's security requirements can be addressed with Transport Layer Security (TLS).
This work proposes to use MQTT secured with TLS for an HEMS's communication. MQTT's network performance is measured in clean conditions for two phases: For connection initiation, the metrics establishment time, data transmitted, and computational effort are quantified. The metrics for the connected phase are latency, throughput, and overhead. Finally, MQTT and TLS are evaluated for the implementation of an HEMS.