Abstract

The Internet of Things (IoT) comprises resource-constrained devices connected to the Internet, interacting with the real world within a wide range of applications. The recent large-scale commercialisation of these low-powered devices has lead to significant security concerns. Message Queue Telemetry Transport (MQTT) is the most widely used application-layer protocol over IoT. A robust and lightweight security scheme is required for use with this protocol, as the security aspect has been omitted from the protocol design. Transport Layer Security (TLS) is recommended in this scenario, though it is often unsuitable due to its resource-intensive nature and lack of end-to-end security provision. A scheme has been proposed using symmetric-key payload encryption, designed entirely over the MQTT protocol. This solution requires minimal overhead on the IoT device, offloading the bulk of the resource-intensive computation onto a central Key Management Service. Overhead is minimised with regard to bandwidth, time-to-idle, memory and computation, and improves upon TLS in all of these areas. The scheme successfully provides secure and authenticated end-to-end communication between clients in the system.