要 旨

ワンタイムパスワード認証方式 SAS-2 を用いた IoT 環境向け通信方式

藤原 蓮

現在, IoT 環境において安全な通信を実現する方式として MQTT over SSL/TLS が挙げられる．これは, SSL/TLS によって提供される安全な接続の上で, MQTT 通信を行う方式である．この方式では, 認証処理及び共通鍵の共有に, 処理負荷が重い公開鍵暗号方式を使用している．従ってクライアントのリソースに制限があることが想定される IoT 環境では, 負荷による影響が大きく, 処理時間が増加するという問題がある．この問題を解決するために本稿では, 認証時と共通鍵の共有時にワンタイムパスワード認証方式 SAS-2 を用いる MQTT over SAS の提案を行う．また, クライアントにおける負荷という観点から既存方式との比較を行い有用性を示す．

キーワード　IoT, MQTT, SSL/TLS, SAS , 認証, 鍵共有, 公開鍵暗号方式

Abstract

A communication method over SAS-2 for the IoT environment

MQTT over SSL/TLS is known secure communication method for the IoT environment. That is MQTT communication on the safe connection offered by SSL/TLS. However, This method use public key cryptosystem of a weighty load for authentication and key exchange. Client's devices are more affected by weighty load, because resources is subject to restrictions by the IoT environment. Therefore there is a problem of increased processing time. In this thesis, I propose a new method which solves such problem. The new method applies SAS-2 to authentication and key exchange. In addition, I compare new method and applied SSL/TLS method to show utility.

key words IoT, MQTT, SSL/TLS, SAS , Authentication, key exchange, public key cryptosystem