EAI Endorsed Transactions
on Internet of Things

Research Article EAI.EU

Securing Communication in MQTT enabled Internet of Things with Lightweight security protocol

Adil Bashir and Ajaz Hussain Mir

Department of Electronics and Communication Engineering
National Institute of Technology Srinagar, Jammu and Kashmir, India-190006
Email: adilbashir.445@gmail.com

Abstract

This paper proposes a security algorithm for Internet of Things (IoT) using simple lightweight cryptographic operations. The main advantage of the proposed algorithm is the simplicity, energy efficiency and the speed of algorithm such that it can be computed quickly using a low-power microcontroller. The encryption of the sensed data is performed using simple operations so as to consume smaller amount of node energy. To test the effectiveness, of the proposed algorithm, an experimental rig is set up to implement the proposed algorithm. The analysis confirms that the proposed algorithm provides end-to-end encryption and imparts security against likely attacks such as brute force attack, spoofing attack, and has small code footprint. It is envisaged that the algorithm can be very useful in securing message transmissions in Internet of Things.

Keywords: Internet of Things (IoT), Constrained Application Protocol (CoAP), Message Queuing Telemetry Transport (MQTT), IoT Security, MQTT Broker.

Received on 17 June 2017, accepted on 08 August 2017, published on 06 April 2018

doi: 10.4108/eai.6-4-2018.154390

1. Introduction

Internet of Things (IoT) is rapidly gaining popularity due to its potential to bring global digital revolution and is being increasingly used in industrial, transportation, digital health and agricultural applications [1]. With numerous applications, IoT brings lot of research challenges that include having a requisite architecture for control and communication among devices [2] Miniaturization of Components [3], Interoperability [4], Service Orchestration [3], Security & Privacy [5, 6], Standardization [7], etc. IoT being resource constrained network demands lightweight protocols at each layer of Internet Engineering Task Force (IETF) defined protocol stack [8]. The application layer protocols are considered as building-blocks to achieve the expected requirements (e.g. scalability, reliability, performance) in Internet of Things environment. The commonly used protocols at application layer of IoT are Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transport (MQTT) being simple and lightweight protocols.

Among the research challenges presented above, security and privacy is considered as one of the main hindrance for the widespread growth and adoption of IoT as there is no public confidence that IoT will not cause harm to user privacy. The security algorithm for IoT need to take care of several issues that include protecting user privacy, consuming less energy for the process and providing strong security against attacks.

Security mechanisms at each layer of IoT protocol stack [8, 2] are implemented to safeguard the sensed information from adversaries. For example, at link layer, encryption algorithms at the hardware in IEEE 802.15.4 sensing platforms are used to provide security features, for instance in TelosB motes, Advanced Encryption Standard (AES) is used as a symmetric cryptosystem at link layer. However, the encryption mechanisms at link-layer only safeguards hop-to-hop communication and the messages on an IP network are not protected from adversaries. At network layer, IPSec [9] is used to provide security related services. But employing IPSec induces