International Journal of Security and Its Applications
Vol. 11, No. 11 (2017), pp.53-66
http://dx.doi.org/10.14257/ijsia.2017.11.11.05

Securing Publish-Subscribe Services with Dynamic Security Protocol in MQTT Enabled Internet of Things

Adil Bashir and Ajaz Hussain Mir

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

Abstract

Rapid developments in the field of embedded system, sensor technology, IP addressing and wireless communication are driving the growth of Internet of Things (IoT) in a variety of applications which include environment monitoring, smart manufacturing, e-health and smart agriculture. Due to heterogeneous and constrained nature of IoT nodes, many new security and privacy issues are introduced. IoT devices and systems collect a lot of private data about people, for example an intelligent meter knows when you are home and what devices you use when you are there. This data is shared with other devices and also stored in database or cloud server. Absence of security protocols for these resource constrained smart devices averts their widespread implementation. To address this problem, we propose a mechanism for securing application layer MQTT (Message Queue Telemetry Transport) protocol messages in IoT. The proposed security method for Internet of Things is lightweight in nature and suits well for resource constricted devices. The proposed method counters most of the likely confidentiality attacks in IoT.

Keywords*: Internet of Things (IoT), Message Queue Telemetry Transport (MQTT), MQTT-SN (for Sensor Networks), Data Distribution Service (DDS), Constrained Access Protocol (CoAP)*

1. Introduction

Internet of Things involves connecting physical objects to the internet, making them locatable and reachable remotely in the virtual domain [1, 2, 3]. Internet of Things (IoT) is regarded as the third wave of global information industry, steam-powered print technology and electronic communications being the other two in the list [4]. IoT is beginning to grow drastically, as consumers, business organizations and governments perceive the advantage of connecting inert devices to the internet. Approximately 20.8 billion connected things will be in use worldwide by the end of 2019, up 41 percent from 2017 and will reach 50 billion by 2020 [5]. The IoT will result in $1.7 trillion in value added to the global economy in 2019 [6]. IoT has distinct characteristics from those of existing Internet environments in a way that it is comprised of resource constrained devices, where the resources include CPU, memory, and battery.

To make IoT into a realization many key challenges exist, for example, security and privacy issues, client interaction, development of Application Program Interfaces (API) [7]. These challenges need to be addressed for widespread implementation and adoption of Internet of Things. Among the research challenges mentioned above, security and privacy issues are considered as obstruction for the adoption of IoT because there is no assurance that IoT will not detriment user privacy. This can be done by tailoring existing security protocols to make them suitable for resource constricted IoT nodes or develop

Received (July 10, 2017), Review Result (November 6, 2017), Accepted (November 16, 2017)

ISSN: 1738-9976 IJSIA