Powering the Internet of Things with MQTT

By Ming Fong
Senior Principal Development Engineer
Schneider-Electric Software, LLC.

Introduction

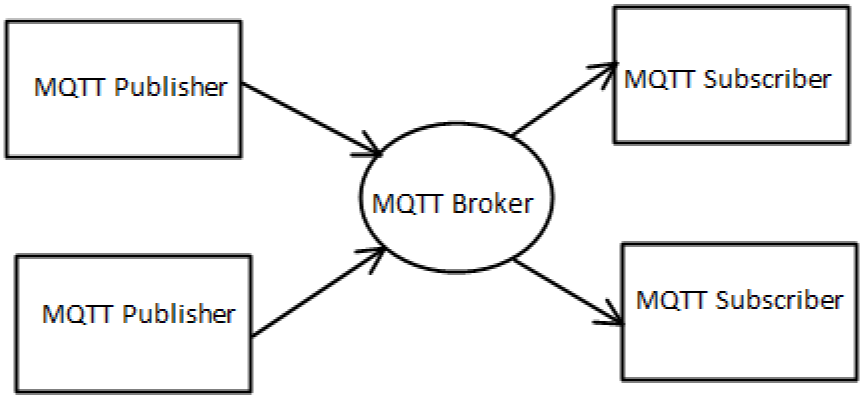
In the last ten years, devices such as smartphones, wearable fitness and health-tracking devices, smart thermostats, small footprint computing devices created a new industry where these devices can connect to each other to provide data and information that was previously deemed expensive to obtain. This new industry is the internet of things (IoT). The internet of things handles machine to machine (M2M) communication. It is a network of data collection devices. It involves the inter-networking of devices (things) to enable data and information to be collected and reported at the desired time and location. Devices connecting to IoT are usually portable and mobile. Some devices may be situated in remote locations where data collection is crucial but accessibility to public infra-structure such as electricity may be limited. Commerce and industry seeing the benefit of IoT is gradually bracing the use of IoT devices. This includes transportation, agriculture, industrial automation and remote data acquisition. One characteristic for these devices is that they are low cost and they consume very little power. This is primarily driven from the portability and "remote-ness" of the device. MQTT is a communication protocol designed with this in mind. Even though MQTT was designed prior to this age of IoT, its characteristics meet the requirements of IoT and therefore have full advantage of being adopted into the IoT space. This paper provides an insight into the MQTT protocol.

What is MQTT

MQTT stands for Message Queueing Telemetry Transport. It is a publish-subscribe messaging protocol designed for machine to machine communications. It is portable and can run different hardware platforms and software environment. It can be integrated into different operating environments – mobile, desktop, embedded. It is lightweight and thus advantageous for integrating sensor data with system devices or computer with low power consumption requirement.

Characteristics of MQTT Protocol

1. Publish-Subscribe Model



MQTT uses the publisher-subscriber model for communications. A broker is used as an intermediary between the publishers and subscribers. The data source publishes the data to the broker. The broker is situated in an environment where accessibility to the network and electrical power is not a constraint. The broker forwards the message to the subscribers. Communication between the broker and its client (publisher or subscriber) uses a typical client/server approach. This is a very scalable connectivity model especially in the IoT environment when connected things (devices) do not need to know each other.

2. Message Protocol

The MQTT protocol is an application protocol. It is used on top of the TCP transport protocol or WebSockets transport protocol. An MQTT message consists of a fixed header, a variable header, and a payload. The header length is typically less than 10 bytes long and is one of the very few communication protocols with very low overhead. The maximum length of the payload is 256 MB. MQTT does not prescribe any payload format. The content of the message is solely determined by the publisher. Text or graphical data can be transmitted as the payload of the protocol. There are only four categories of control packets that arbitrate the communication between the MQTT broker and its clients.

- Connect and Disconnect
  Control packets to establish the connection and disconnection between the broker and its clients.

- Publish
  MQTT publisher sends the message to the broker.

- Subscribe and Unsubscribe
  MQTT brokers forward the received message from the published to a list of subscribers.

- Ping

MQTT publisher-subscriber sends this packet to the broker to indicate that it is still alive and to exercise the network connectivity.

3. *Message Content*

Messages in MQTT are identified by the publisher with a "topic". A subscriber indicates the interest of a message from the publisher by subscribing to the data labeled with the appropriate topic. The MQTT specification also prescribes topic filters to be hierarchical with wildcard capability to allow the subscriber high flexibility in subscribing to wide set of topics.

4. *Message Delivery*

Another unique feature for MQTT is in the handling of delivery of messages. The MQTT protocol specifies a set of control bits in the control packet to ensure delivery of a message is made based on the need of the MQTT client.

Quality of Service (QoS)

There are 3 defined levels of QoS to assure the delivery of a message. The QoS value is set by the publisher when sending a message and by a subscriber when receiving a message. If the two QoS settings do not match, the broker will resolve the QoS requirement as required.

QoS value	Description	Delivery
0	At most once delivery	Fastest but message may be lost if receiver is not available. Sender does not cache the message. Suitable for repetitive data messages.
1	At least once delivery	Sender of message will cache the sent message until it is acknowledged by the receiver. Message is transmitted and re-transmitted until it is acknowledged by the receiver.
2	Exactly once delivery	Most secure but slowest in delivery. Message delivery is arbitrated between the sender and receiver so that the message will be sent only 1 time.

Retain Message

A publisher can optionally mark a message as "retained" to ensure its delivery to subscribers. Once a message with the retain flag marked by a publisher, the broker will forward the messages to any current subscribers and to retain the message so that any new subscriber connected to the broker will still receive it. For the broker to retain the last message sent from the publisher, the publisher will set the message QoS value to 0 and retain flag to 1.

Will and Last Testament Message

Any MQTT client (publisher of subscriber) can update its connection state by sending a Will message to the broker. Upon determining that the client has exited or disconnected, the broker will send the 'will' message to any subscribers interested to the state of the client. In a typical industrial automation environment, the subscriber can use this message to indicate the equipment or a data point will be offline or will not be available upon receiving this message.

Message Ordering

Messages sent from the publisher are ordered based on the QoS and time order in the broker. The broker will forward the messages to the subscribers in the same order.

5. *Power Consumption and Network Bandwidth*

The following table shows a battery consumption and message throughput comparison of MQTT over SSL against HTTPS on an Android phone.

	3G		Wifi	
	HTTPS	MQTT with SSL	HTTPS	MQTT with SSL
% Battery/Message	0.01709	**0.00010**	0.00095	**0.00002**
Messages/Hour	1708	**160278**	3628	**263314**
Messages Received per 1024 Sent Messages	240	**1024**	524	**1024**

Source: http://stephendnicholas.com/posts/power-profiling-mqtt-vs-https (Reference 4)

From the above, MQTT messaging is 94 times faster on a 3G network than HTTPS (REST) communication. In terms of power consumption, MQTT uses 170 times less power than the HTTPS (REST) protocol on a 3G network. The simplicity of the MQTT protocol and message structure contributes to its adoption in the IoT environment when network bandwidth and power consumption is a major factor.

6. *Security*

Security in MQTT is considered in two aspects:

- Authentication

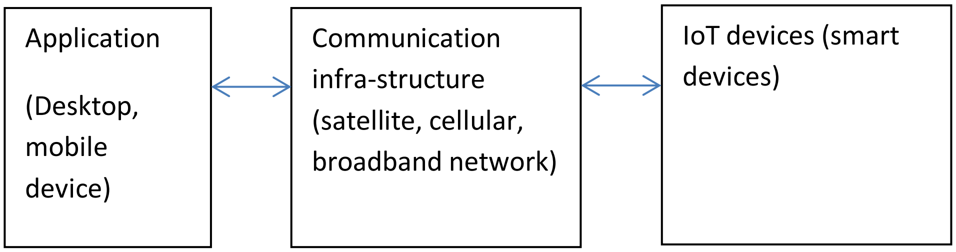
  Authentication is the act of confirming the integrity and privacy of MQTT data transmitted between the MQTT client and broker. MQTT supports the Transport Level Security Protocol (TLS) for authentication. TLS is commonly used in secured consumer and commercial internet communication. The TLS protocol ensures that there is no man-in-the-middle threat and that the client is indeed communicating to the desired broker.

- Identification

  In each MQTT connection, the client has to provide its identification to the broker or requests it to be auto-generated by the broker. The identification is meant to uniquely identify the client during communication. Username and password fields are also provided in the protocol to allow the broker to identifying the caller and authorize the access of appropriate resources.

Applying MQTT

As long as there is a sensor that collects data, the MQTT protocol can be considered as a choice. Because of its low communication bandwidth requirement, MQTT is most suitable in telemetry applications and mobile devices where accessibility, network bandwidth and power consumption are the major factors. Due to its simplicity and availability in multiple operating systems and devices, applications using MQTT can be deployed to desktop application, mobile devices, Edge Gateways and embedded devices.


Application
(Desktop, mobile device)
Communication infra-structure (satellite, cellular, broadband network)
IoT devices (smart devices)

Here are a few examples of use cases where MQTT is applicable.

- Healthcare
  Physicians can use MQTT devices to monitor home-care patient’s medical conditions.

- Data Logging
  Electric or gas meter reading can be sent to the central office periodically.

- Mobile Devices
  Applications employ MQTT to provide instant messaging, mobile reporting and location tracking.

- Pipeline Monitoring
  Pipeline data can be collected and sent via MQTT to edge gateways at a fraction of cost of the traditional approach.

- Preventive Maintenance and Predictive Maintenance

Machinery conditions in the factory can be reported via MQTT gateway to traditional backend servers to support preventive and predictive maintenance of machinery.

- Automotive
  GPS location and engine conditions can be reported to the manufacturer for real time diagnosis.

- Fleet Management
  Location and routing of vehicles can be made in real time to achieve optimal throughput

Things Will Only Get Better

In October 2014, the MQTT protocol specification was ratified as an OASIS Standard. In April 2016, the MQTT standard was formally adopted by ISO and IEC committees as standard for Internet of Things. This will encourage even higher adoption with more things (devices) built with this protocol.

In 2016, it was estimated there are over 6.4 billion connected devices. By 2020, there will be over 20 billion connected devices. (Reference 3) By 2025, there will be over 50 billion devices.

MQTT will continue to make digitization of information easier as the industry is continuing its pursuit of better technology and infrastructure support for IoT. The IoT environments will be demanding higher data throughput, lower power consumption, low latency, high reliability and highly secured communication. Ongoing development is already taking place, such as 5G Network, HaLow Wifi, multi-antenna wireless technology. They all target these IoT requirements.

With the proliferation of IoT devices originating in the consumer-focused industry, business and industrial automation processes will also change. As these technologies allow devices to be connected together easily and daily, the industrial automation ecosystem can leverage these devices to provide additional information that was not possible even 10 years ago. Industrial automation will not be just confined to sensors and instrumentation hardwired in the factory floor, it might involve information collected from remote sensors, from web services in the internet, and from consumers directly. Initiatives in the industrial automation and manufactory industries leveraging industrial internet of things (IIoT) are already taking place. Industrie 4.0 will bring another industrial revolution by leveraging the IoT capabilities to change existing industrial automation and manufacturing processes and practice. Fog Computing will improve the delivery time of data and information to the consumers. Human beings and machines will be connected and information will flow through this world from sensors to boardrooms to consumers. The MQTT protocol will be deeply embedded into such communication infrastructure providing data and information to everyone.

References

1. The MQTT specification can be found in http://mqtt.org.
2. The OASIS consortium has various articles concerning cyber-security on MQTT: http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/mqtt-nist-cybersecurity-v1.0.html
3. Source: http://www.gartner.com/newsroom/id/3165317
4. Source: http://stephendnicholas.com/posts/power-profiling-mqtt-vs-https