Protocolo MQTT para sistemas de IoT

Um estudo técnico/prático

Larissa L. Wong
Marco A. G. Pedroso
Victor E. Almeida

UNIOESTE

3 de maio de 2022

Conteúdo

Criação do Protocolo

Começou a ser projetado durante a década de 1990 por:

Figura 1: Andy Stanford-Clark da IBM

Figura 2: Arlen Nipper da Cirrus Link/Eurotech

Problemas a serem resolvidos

- Resolver o problema de conexão de oleodutos via satélite.
- Limitações:
  - Alta latência;
  - Baixa largura de banda;
  - Dispositivos com pouca bateria.

Requisitos do Protocolo

- Implementação simples;
- Uso de QoS, *Quality of Service* por quem publica a mensagem;
- Uso eficiente de largura de banda, baixo *overhead*;
- Baixo custo energético para envio;
- Possibilidade de enviar qualquer tipo de dado;
- Possibilidade de manter conexões ativas, prontas para enviar e receber dados;

Fase do protocolo proprietário

- Primeira versão implementada no ano de 1999;
- Batizado MQTT, *MQ Telemetry Transport*, em referência ao produto da IBM MQ Series
- Muito utilizado embarcado em produtos da IBM.

Fase do protocolo aberto I

- Demanda/Aplicabilidade IoT;
- Em 2010 o protocolo se tornou livre;
- Primeira versão lançada 3.1;
- Investimentos da IBM através da Eclipse Foundation para criar um ecossistema em torno do protocolo.

Fase do protocolo aberto II

Figura 3: Exemplos de aplicações do ecossistema MQTT

Fase do protocolo aberto III

- No ano de 2013 a IBM buscou padronização com a OASIS;
- 29 de outubro de 2014 o MQTT foi aprovado como padrão pela OASIS na sua versão 3.1.1

Fase atual do protocolo

- A última versão 5.0 março de 2019;
- Funcionalidades modernas como:
  - facilidade de conexão e interação com a nuvem;
  - Tratamento de erros;
- Implementações de clientes para diversos sistemas e linguagens;
- Implementação de diversos brokers;
- Utilizado por grandes empresas tanto software aberto quanto proprietário.

Aplicações em IoT

- Uso Doméstico e Educacional
- Uso Industrial
  - BMW Mobility Services
  - Matternet Autonomous Drones

BMW Mobility Services

- Drive Now;
- Serviço de compartilhamento de veículos;
- Realização de tarefas de modo remoto;
- Presença em 12 cidades na Europa;
- Uso do protocolo MQTT;

Matternet Autonomous Drones

- Drones para transporte de amostras;
- Obrigatoriedades legais;
  - Monitoramento dos voos
  - Acesso em tempo real a dados
  - Controle remoto dos drones
- Uso do protocolo MQTT;

Embasamento teórico - Cliente I

Cliente: programa ou dispositivo que irá enviar ou receber informação. Nesse sentido o cliente deve ser capaz de:

- iniciar uma conexão com o servidor,
- realizar a publicação de informações em tópicos,
- realizar a subscrição a tópicos de interesse,
- realizar o cancelamento de uma subscrição e,
- finalizar uma conexão com o servidor.

Embasamento teórico - Broker I

Broker: programa ou serviço que intermediá e gerência a informação, o envio e recebimento de dados dos clientes, é comum se referir ao mesmo como servidor. Nesse sentido o servidor deve ser capaz de:

- gerencia as conexões como os clientes,
- gerenciar as mensagens publicadas pelos clientes,
- gerenciar as subscrições dos clientes e,
- retransmitir as mensagens recebidas aos clientes.

Embasamento teórico I

- **Conexão de rede**: se refere ao serviço provido pelo protocolo de comunicação na camada subjacente (TCP/IP) ao protocolo MQTT, e que permite o envio de informação entre os dispositivos.
- **Mensagem**: representa a informação que se deseja transmitir e que portanto constitui o objetivo da comunicação. De forma geral, e pelas caraterísticas do protocolo, a mensagem deve ocupar o mínimo espaço possível - na maioria dos casos é um único valor.

Embasamento teórico II

- **Sessão**: se corresponde com o período de interação entre um cliente e um servidos, durante o qual é mantido um grupo de informações que representam o estado da comunicação, podendo ser composto por mais de uma conexão.
- **Subscrição**: é o ato de que o cliente desempenha para indicar ao servidor interesse em receber atualizações sobre a mudança de um tópico. Dessa forma, uma subscrição se encontra composta por um Filtro de Tópicos, para um ou mais tópicos, e um valor indicando a Qualidade de Serviço deseja (QoS).

Embasamento teórico III

- **Subscrição compartilhadas**: são subscrições que se encontram associadas com mais de uma sessão de comunicação entre o cliente e o servidor. Dessa forma, permitem um maior rango de padrões de comunicação.
- **Caracteres mágicos**: também chamados de Wildcards, permitem ao cliente indicar interesse em receber notificações de mais um tópico, para isso fazendo uso de caracteres que definem o padrão dos tópicos desejados.
- **Nome de Tópico**: rótulo ou identificador de uma informação específica dentro do broker e que é constantemente atualizada pelos cliente quando publicam uma nova informação no tópico.

Embasamento teórico IV

- **Filtro de Tópico**: é uma expressão contida numa subscrição é que se corresponde com um ou mais tópicos
- **Paquete MQTT**: conjunto de informação útil à comunicação cliente-servidor envida através da conexão de rede. O protocolo MQTT especifica 15 tipos de pacotes diferentes, os quais serão especificados a continuação.

Estrutura básica dos pacotes

Tabela 1: Estrutura básica comum a todos os pacotes MQTT.

Cabeçalho fixo
Cabeçalho variável
Carga útil

Estrutura do cabeçalho fixo

Tabela 2: Estrutura do cabeçalho fixo utilizado no protocolo MQTT.

Bit	7	6	5	4	3	2	1	0
Byte 1	Tipo de pacote MQTT				Sinais específicos do pacote			
Byte 2	Espaço restante							
. . .								

Sinais específicos do pacote: complementa a informação do tipo do pacote.
Espaço restante: informação útil e de controle dependentes de cada tipo de pacote.

Tipos de pacotes

Tabela 3: Tipos de pacotes utilizados pelo protocolo MQTT – Parte I.

Tipo	Código	Remetente	Descrição
Reserved	0	-	Reservado
CONNECT	1	Cliente	Solicitação de conexão
CONNACK	2	Servidor	Confirmação de conexão
PUBLISH	3	Ambos	Publicar mensagem
PUBACK	4	Ambos	Publicar confirmação (QoS 1)
PUBREC	5	Ambos	Publicar recebimento (QoS 2 – parte 1)
PUBREL	6	Ambos	Publicar lançamento (QoS 2 – parte 2)
PUBCOMP	7	Ambos	Publicar conclusão (QoS 2 – parte 3)

Tipos de pacotes

Tabela 4: Tipos de pacotes utilizados pelo protocolo MQTT – Parte II.

Tipo	Código	Remetente	Descrição
SUBSCRIBE	8	Cliente	Solicitação de inscrição
SUBACK	9	Servidor	Confirmação de inscrição
UNSUBSCRIBE	10	Cliente	Solicitação de cancelamento de inscrição
UNSUBACK	11	Servidor	Confirmação de cancelamento de inscrição
PINGREQ	12	Cliente	Solicitação de PING
PINGRESP	13	Servidor	Resposta de PING
DISCONNECT	14	Ambos	Notificação de desconexão
AUTH	15	Ambos	Troca de autenticação

Tipos de pacotes I

- **CONNECT - Requisição de Conexão**
- **CONNACK - Reconhecimento de conexão**
- **PUBLISH - Publicar mensagem**
- **PUBACK - Reconhecimento de publicação**
- **PUBREC - Recebimento de publicação**
- **PUBREL - Liberação de publicação**
- **PUBCOMP - Publicação completada**
- **SUBSCRIBE - Requisição de subscrição**

Tipos de pacotes I

- **SUBACK - Reconhecimento de subscrição**
- **UNSUBSCRIBE - Requisição de cancelamento de subscrição**
- **UNSUBACK - Reconhecimento de cancelamento de subscrição**
- **PINGREQ - Requisição de PING**
- **PINGRESP - Resposta a uma Requizição de PING**
- **DISCONNECT - Requisição de desconexão**
- **AUTH - Intercambio de autentificações**

Fatores de Risco

- Grande quantidade de dispositivos IoT
- Baixo suporte para mecanismos de segurança convencionais
- Ataques DDoS
- Roubo de informações
- Obtenção do controle dos dispositivos

Ataques DDoS - Distributed Denial of Service

- Um dos tipos de ataques mais comuns
- Interrupção no tráfego de servidores, serviços ou rede por meio de grande fluxo de pacotes;
- Botnets;
  - Dispositivos infectados por malware
- Dificuldade na verificação contra botnets;

Soluções para Diminuição dos Riscos

- Realização de autenticação;
- Uso de algoritmos e protocolos de criptografia;
- Uso de VPN;
- Detecção de atividades suspeitas;
- Secure MQTT
  - TLS - Transport Layer Security
  - Utilização da porta 8833
  - Formato de uso cadastrado na IANA (Internet Assigned Numbers Authority)

Dispositivos e softwares da parte prática

- Esp32:
  - Sensor Adafruit BMP-280;
  - Led embutido no Esp32;
  - C/C++ (Framework Arduino e ESP-IDF);
- Raspberry:
  - Docker executando o broker mosquitto;
  - Cliente inscrito no tópico “#”

Diagrama da aplicação

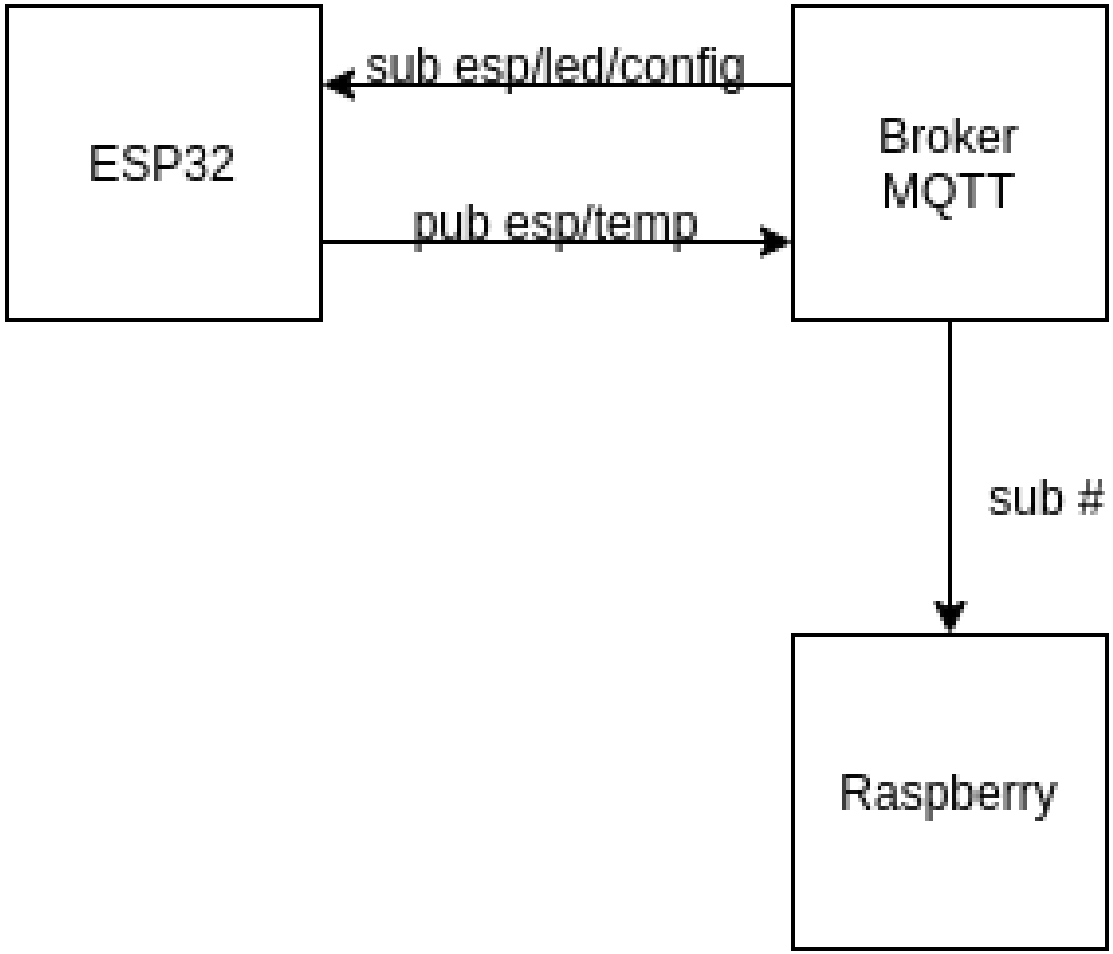

Figura 4: Dispositivos e tópicos utilizados

Códigos Fonte I

```
1  void setup() {
2      if (!sensor.begin(BMP280_ADDRESS)) {
3          if(!sensor.begin(BMP280_ADDRESS_ALT)) {
4              delay(1000);
5              ESP.restart();
6          }
7      }
8      pinMode(LED_PIN, OUTPUT);
9      wifiConnect();
10     MqttConnect();
11     xTaskCreate(taskSendTemperature, "send",
           20000, NULL, 1, &handle);
12 }
```

Códigos Fonte II

```
13
14  void loop() {
15      if (!mqttClient.connected()) {
16          MqttConnect();
17      }
18      mqttClient.loop();
19  }
```

Mão na massa!!

Agradecimentos

Perguntas?

Obrigado pela atenção