A Review of Application Protocol Enhancements for Internet of Things

Fatma Hmissi[1] Sofiane Ouni[2]

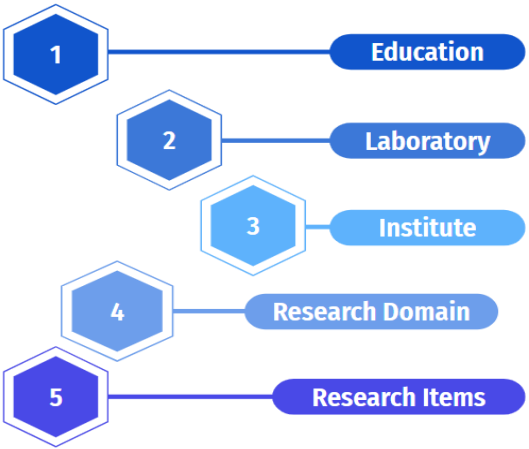
[1, 2] Cristal Laboratory, National School of Computer Scinces (ENSI)

[1] fatma.hmissi@ensi-uma.tn, [2] soufiane.ouni@insat.rnu.tn

UBICOMM 2021

October 03, 2021 to October 07, 2021 - Barcelona, Spain

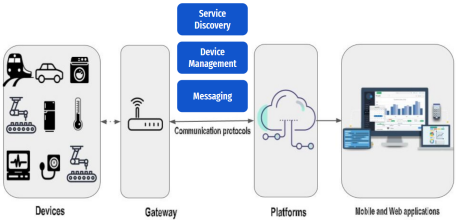
About Me - Fatma Hmissi



Contents I

Introduction

- The Internet of Things (IoT) is an innovative technology.
- The Internet of Things easies the people's lives and businesses way in many areas.
- The Internet of Things systems have no standard architecture.

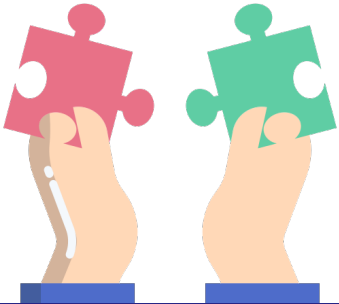


Communication Protocols

- Allow the connectivity.
- Exchange messages between physical or virtual entities,e.g., devices and Cloud, by defining rules and constraints where several requirement must be taken by these protocols in order to succeed IoT systems.

Contributions

1. Overview the initial communication protocols adopted for :
   - **Messaging**
   - **Device Management**
   - **Service Discovery**
2. Identify the problems most studied by the existing protocols in IoT scenarios.
3. Review of the studied solutions that improve existing protocols.



IoT Application Layer Protocols

Data

A Messaging protocol ensure communication between entities, it enable exchanging data between the components of a IoT systems.

Device Management

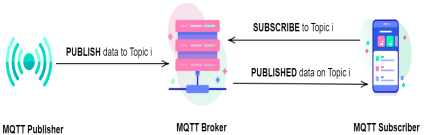
A device management protocol enables the abstraction of an IoT/M2M device as a managed object to make the management of the device much easier.

Service Discovery

Service discovery protocols (SDPs) are communication protocols that provide mechanisms to help clients to discover services available on the network.

Messaging Protocols (1/4)

- Most relevant messaging protocols:
  - Message Queuing Telemetry Transport (MQTT)
  - Constrained Application Protocol (CoAP)
  - Data Distribution Service (DDS)
  - Advanced Message Queuing Protocol (AMQP)
  - the eXtensible Messaging and Presence Protocol (XMPP)
  - Hypertext Transfer Protocol (HTTP)
- Message Queuing Telemetry Transport (MQTT)

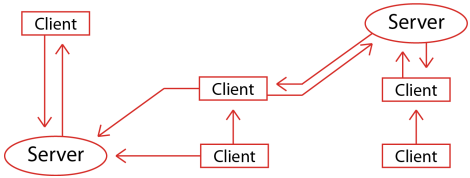


MQTT's message exchange

1. Multiple clients connected to a central broker (MQTT Broker).
2. MQTT clients' act as senders and receiver of messages.
3. Every time the MQTT Broker get a new publish message to a specific topic, he broadcasts this message to the entire subscribed receivers.

Messaging Protocols (2/4)

- Constrained Application Protocol (CoAP)



CoAP's message exchange

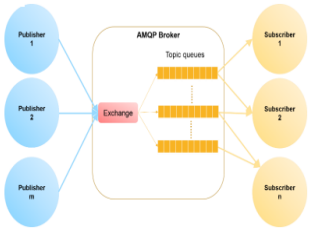
1. multiple clients connected to a multiple servers.
2. Each client sends a request using an URI (Uniform Resource Identifier) to the server with GET, POST, PUT and DELETE actions.
3. GET and POST are used to retrieve and send data to server.
4. PUT is used to update and do changes to resource data.

Messaging Protocols (3/4)

- Advanced Message Queuing Protocol (AMQP)

AMQP's message exchange

- AMQP has three components, Publishers, Subscribers and, both parts of an AMQP Broker are Exchanges of Message queues.
- The Publisher creates a bare message and sends it to the Exchanges components that are used to forward the messages to appropriate message queues using the routing keys contained in messages, these latters can be stored into message queues before forwarding it to Subscribers.



Messaging Protocols (4/4)

- Messaging protocols main features :

Feature		MQTT	CoAP	AMQP	XMPP	DDS
Interaction	Publisher-Subscriber	✓		✓	✓	✓
	Request-Response		✓			
Transport	TCP	✓		✓	✓	✓
	UDP		✓			
Architecture	Centralized	✓		✓		
	Decentralized		✓		✓	✓
Scope	device-to-device		✓	✓		
	device-to-Cloud	✓		✓	✓	
	Cloud-to-Cloud	✓		✓	✓	
Devices supported	Constrained	✓	✓		✓	
	Powerful			✓		✓

Device Management Protocols

- Most popular device management protocols for IoT:
  - Open Mobile Alliance Device Management standard (OMA-DM)
  - Lightweight M2M (LwM2M)
  - The Broadband Forum defined CPE WAN management protocol (CWMP)
- Most metrics and disadvantages of Device Management Protocols

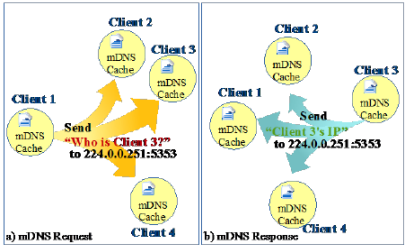
Features	OMA-LwM2M	OMA-DM	TR-069
Client-server architecture	√	√	√
Telecommunication protocol	χ	√	√
Industry protocol	√	χ	χ
Interoperability	√	χ	χ
Inventory	√	√	√
Data collection	√	χ	χ
Provisioning	√	√	√
Authentication	√	√	√
Configuration	√	√	√
Control	√	√	√
Monitoring	√	√	√
Diagnostics	√	√	√
Firmware update	√	√	√
Application data	√	x	x
Security	√	√	x
Constrained device	√	x	x
Mobile devices	√	√	x
Fixed devices	√	X	√
IP connected devices	√	X	x
NAT system	√	√	√
FW system	√	√	-
Cellular technology	√	√	√
WIFI technology	√	χ	-
Structured data	√	√	√ (height)
XML serialization format	χ	√	√
Binary serialization format	√	χ	χ
Plain Text serialization format	√	χ	χ
TLV serialization format	√	χ	χ
JSON serialization format	√	χ	χ
CoAP/UDP	√	χ	χ
CoAP/SMS	√	χ	χ
MQTT/TCP	χ	χ	χ
Support use of multiple Servers	√	√	√

Service Discovery Protocols (1/2)

- Multicast Domain Name System (mDNS)
  - Open protocol defined by IETF.
  - Requires minimal configuration. based on the Internet.
  - Protocol (IP) and the User Datagram Protocol (UDP).

How mDNS works

1. mDNS client send IP multicast message to all the nodes in the local domain to ask devices that have the given name to reply back.
2. The target machine it multicasts a response message which contains its IP address when it receives its name.
3. All nodes in the network receiving the multi-cast message of the target machine update their mDNS caches accordingly.



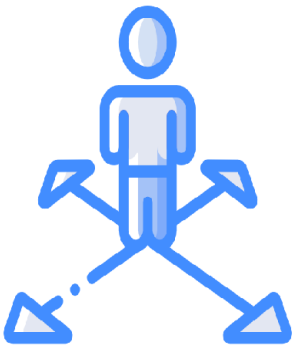
Service Discovery Protocols (2/2)

- Simple Service Discovery Protocol (SSDP)
  - Open protocol
  - Based on IP, UDP, and SOAP (Simple Object Access Protocol).

How SSDP works

1. The SSDP client discovers SSDP services by multi-casting a discovery request to the SSDP multicast channel and port.
2. SSDP services listen to on that channel until receiving a discovery request that matches the service it offers.
3. SSDP services responds using a unicast response.

Application Protocols Challenges (1/2)



Real-time communication

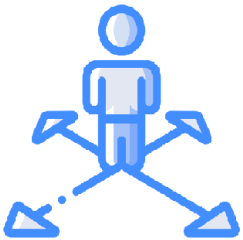
Most IoT solutions involve time constraints to gather and process information, make decisions, and deliver actions that system components must perform. When time restrictions are present, the system is said to be real-time if at least one of the tasks is performed but it must be executed before a certain deadline.

XMPP and DDS protocols are designed for real-time communication.

Constrained devices

IoT devices are constrained. They have limited capabilities, memory, and energy. And the use of heavy communication protocols on these devices reduces the performance of IoT communication. i.e shut down the devices quickly, increase the delay of communication.

Application Protocols Challenges (2/2)



Security

Security is a cybersecurity strategy that prevents unauthorized access to organizational assets including computers, networks, and data.
Application protocols were not designed with security in mind. They are based on common security solutions such as DTLS and TLS.

Interoperability

Interoperability is meant to make communication among heterogeneous devices and software applications from different vendors possible.
OMA-LwM2M support interoperability.

Quality of Service (QoS)

The Quality of Service (QoS) characterizes the quality of communication links between nodes. Generally, it's the capacity to carry the traffic between nodes in the best condition, such as in terms of availability, packet loss rate, and throughput.
CoAP, MQTT, and DDS define different levels of QoS which address different requirements, such as message delivery, timing, loose coupling, and fault tolerance.

Application Protocols Enhancements

Challenge	Focus	Protocol	References
Real-time communication	Industrial application	MQTT	[31]
	IoT based system	MQTT	[50]
	Embedded devices	CoAP	[32]
	Prototype Medical Instruments Applied to Neurodegenerative Disease Diagnosis	MQTT/AMQP	[51]
Constrained devices	Power saving	MQTT	[33], [34]
	Power saving	MQTT-SN	[35], [36]
	Power saving	CoAP	[52]
	Decrease the computational complexity of the clients	MQTT	[53]
Interoperability	Technical Interoperability	MQTT/HTTP	[42]
	Technical Interoperability	MQTT	[43]
	Syntactical interoperability	All protocols	[54]
	Semantic interoperability	MQTT	[44]
Security	Authentication	MQTT/MQTT-SN	[38], [55]
	User authority to information access	MQTT	[39]
	User Registration	MQTT	[56]
	Denial-of-sleep attacks	CoAP	[40]
Quality of services	Control the traffic flow between the subscribers and publishers	MQTT	[45], [46]
	Maintain message order	MQTT	[48]
	Transit urgent message first	MQTT	[47]
	Reduce the delivery of unnecessary messages	MQTT	[49]
	Data Delivery in Mobile Scenarios	MQTT	[57]
	Network Congestion Control	CoAP	[58]
	Object Discovery	CoAP	[58]

Conclusion (1/1)

- The application protocols are subdivided into three types :
  - **Messaging**
  - **Device Management**
  - **Service Discovery**
- The main Challenges facing application protocols in IoT are ;
  - **Real-time communication**
  - **Security**
  - **Quality of Service**
  - **Constrained devices**
  - **Interoperability**

Conclusion (1/2)

The aim of enhanced application protocols is to :

- improve real-time communication by decreasing the delay of communication between IoT devices.
- support interoperability by ensure technical and semantic interoperability.
- improve the security level to reduce the state of risk on IoT devices, IoT data.
- improve the QoS by providing applications policies to control a wide set of non-functional properties, such as data availability, data delivery, data timeliness and resource usage.
- save devices resources by saving power and memory.

Thank You!

Any Question ?