Fog & Edge Computing

Rushikesh Dumbre

I. Introduction

- There is large volume, variety and velocity in the data generated by IOT
- To transfer all the data to the data center for processing is very slow and requires large bandwidth
- Edge computing devices are closer to IOT devices that handle all the necessary processing
- Fog computing includes the edge devices as well as the network infrastructure to transfer data to data centres
- Fog computing brings cloud closer to the IOT devicesy

II. DataLink Protocols

A. IEEE 802.15.4

- It defines a frame format, headers including source and destination addresses, and how nodes can communicate with each other.
- The frame formats used in traditional networks are not suitable for low power multi-hop networking in IoT due to their overhead.
- In 2008, IEEE 802.15.4e was created to extend IEEE 802.15.4 and support low power communication.
- It uses time synchronization and channel hopping to enable high reliability, low cost and meet IoT communications requirements.

1) Slotframe Structure::

- IEEE 802.15.4e frame structure is designed for scheduling and telling each node what to do.
- A node can sleep, send, or receive information. In the sleep mode, the node turns off its radio to save power and stores all messages that it needs to send at the next transmission opportunity.
- When transmitting, it sends its data and waits for an acknowledgment.
- When receiving, the node turns on its radio before the scheduled receiving time, receives the data, sends an acknowledgement, turn off its radio, delivers the data to the upper layers and goes back to sleep.

2) Synchronization::

- Synchronization is necessary to maintain nodes' connectivity to their neighbors and to the gateways.
- Two approaches can be used: acknowledgment-based or frame-based synchronization.
- In acknowledgement-based mode, the nodes are already in communication and they send acknowledgment for reliability guarantees, thus can be used to maintain connectivity as well.
- In frame-based mode, nodes are not communicating and hence, they send an empty frame at pre-specified intervals (about 30 second typically).

3) Channel Hopping::

- IEEE 802.15.4e introduces channel hopping for time slotted access to the wireless medium.
- Channel hopping requires changing the frequency channel using a pre-determined random sequence.
- This introduces frequency diversity and reduces the effect of interference and multi-path fading.

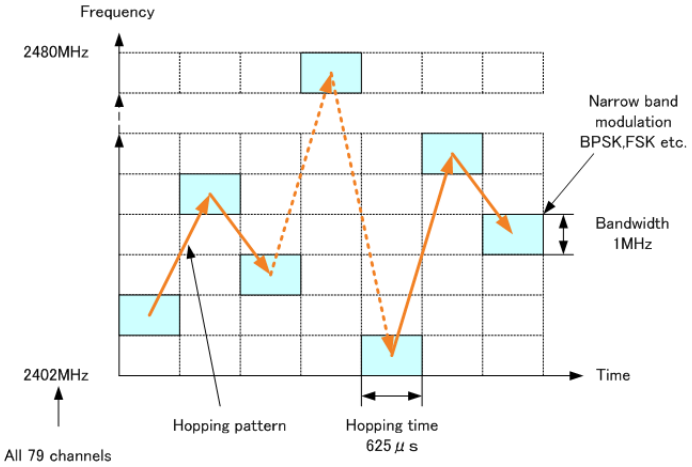

Figure 1. Channel Hopping

4) Network formation::

- Network formation includes advertisement and joining components.
- A new device should listen for advertisement commands and upon receiving at least one such command, it can send a join request to the advertising device.
- In a centralized system, the join request is routed to the manger node and processed there while in distributed systems, they are processed locally.
- Once a device joins the network and it is fully functional, the formation is disabled and will be activated again if it receives another join request.

B. Z-wave

- Z-Wave is a low-power MAC protocol designed for home automation and has been used for IoT communication, especially for smart home and small commercial domains.
- It covers about 30-meter point-to-point communication and is suitable for small messages in IoT applications, like light control, energy control, wearable healthcare control and others.
- It uses CSMA/CA for collision detection and ACK messages for reliable transmission.

- It follows a master/slave architecture in which the master control the slaves, send them commands, and handling scheduling of the whole network.
- A central, network controller, device is required to setup and manage a Zwave network.
- Each Z-Wave network is identified by a Network ID and each device is further identified by a Node ID.
- The Network ID (aka Home ID) is the common identification of all nodes belonging to one logical Z-Wave network.
- Network ID has a length of 4 bytes and is assigned to each device by the primary controller when the device is added into the network.
- Nodes with different Network ID's cannot communicate with each other.
- The Node ID is the address of the device / node existing within network. The Node ID has a length of 1 byte.
- Devices can communicate to one another by using intermediate nodes to route around and circumvent household obstacles.
- A message from node A to node C can be successfully delivered even if the two nodes are not within range, providing that a third node B can communicate with nodes A and C.
- If the preferred route is unavailable, the message originator will attempt other routes until a path is found to the "C" node.
- Therefore, a Z-Wave network can span much farther than the radio range of a single unit; however, with several of these hops a slight delay may be introduced between the control command and the desired result.
- In order for Z-Wave units to be able to route unsolicited messages, they cannot be in sleep mode. Therefore, battery-operated devices are not designed as repeater units.
- A Z-Wave network can consist of up to 232 devices with the option of bridging networks if more devices are required.
- As a source routed static network, Z-Wave assumes that all devices in the network remain in their original detected position. Mobile devices, such as remote controls, are therefore excluded from routing.

C. DASH7

- DASH7 is a wireless communication protocol for active RFID that operates in globally available Industrial Scientific Medical (ISM) band and is suitable for IoT requirements.
- It is mainly designed for scalable, long range outdoor coverage with higher data rate compared to traditional ZigBee.
- It is a low-cost solution that supports encryption and IPv6 addressing.
- It supports a master/slave architecture and is designed for burst, lightweight, asynchronous and transitive traffic.
- Its MAC layer features can be summarized as follows:
  - **Filtering:**
    - Incoming frames are filtered using three processes; cyclic redundancy check (CRC) validation, a 4 -bit subnet mask, and link quality assessment.
    - Only the frames that pass all three checks are processed further.
  - **Addressing:**
    - DASH7 uses two types of addresses: the **unique identifier** which is the **EUI-64 ID** and **dynamic network identifier** which is **16-bit address** specified by the network administrator.
  - **Frame format:**
    - The MAC frame has a variable length of maximum 255 bytes including addressing, subnets, estimated power of the transmission and some other optional fields.

III. Network Protocols

A. RPL

- RPL stands for Routing Protocol for Low-Power and Lossy Networks
- RPL is a distance vector, source routing protocol.
- A distance vector protocol operates on a vector of distances (hop count) to other nodes
- A source routing protocol allows user to specify partial or complete route to the destination
- RPL builds a Destination Oriented Directed Acyclic Graph (DODAG) in which there is only one route from any node to the root node
- Root nodes manage all the data collection and coordination
- When communicating, the node sends a Destination Advertisement Object (DAO) to its parents
- Finally DAO reaches root node and it will decide where to send it.
- When a new node wants to join the network, it sends a DODAG Information Solicitation (DIS) request to join the network and the root will reply back with a DAO Acknowledgment (DAO-ACK) confirming the join.
- Only root has the complete knowledge of the entire DODAG. Hence, all communications go through the root in every case.

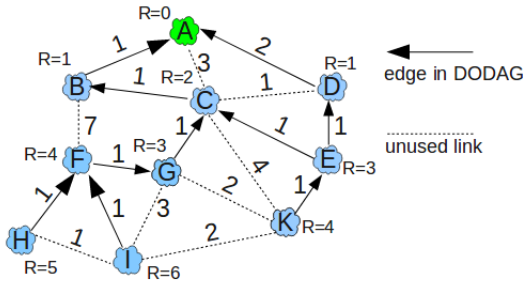

Figure 2. DODAG

IV. Network Layer Encapsulation Protocols

- One problem in IoT applications is that IPv6 addresses are too long and cannot fit in most IoT datalink frames which are relatively much smaller.
- Hence, IETF is developing a set of standards to encapsulate IPv6 datagrams in different datalink layer frames for use in IoT applications.

A. 6LoWPAN

- It stands for IPv6 over Low-power Wireless Personal Area Network
- It is applied to low power devices with limited processing capabilities
- Allows for IPv6 packets to be sent over IEEE 802.15.4

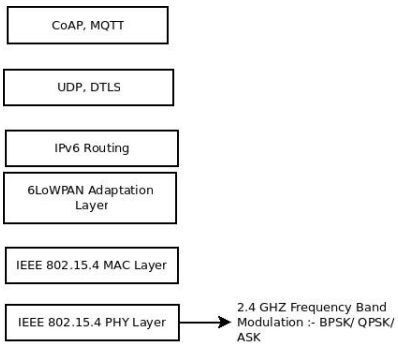

Figure 3. Layers of 6LoWPAN

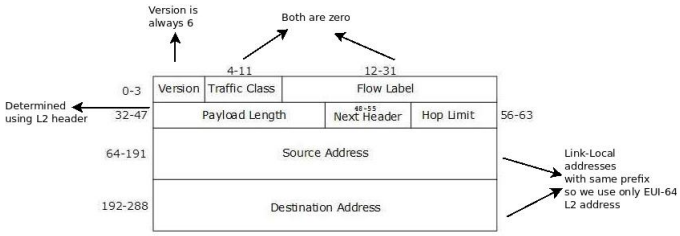

Figure 4. Compression of header

V. Session Layer Protocols

A. MQTT

- Message Queue Telemetry Transport
- Publish/Subscribe decouples a client, which is sending a particular message (called publisher) from another client (or more clients), which is receiving the message (called subscriber).
- In order to determine, which message gets to which client, MQTT uses topics. A topic is a hierarchical structured string, which is used for message filtering and routing.

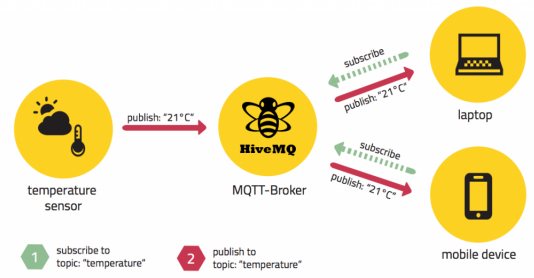

Figure 5. MQTT

- The broker is primarily responsible for receiving all messages, filtering them, decide who is interested in it and then sending the message to all subscribed clients
- Another responsibility of the broker is the authentication and authorization of clients.
- The MQTT connection itself is always between one client and the broker, no client is connected to another client directly.
- The connection is initiated through a client sending a CONNECT message to the broker. The broker response with a CONNACK and a status code. Once the connection is established, the broker will keep it open as long as the client doesn't send a disconnect command or it looses the connection.

B. AMQP

- The Advanced Message Queuing Protocol
- It runs over TCP and provides a publish/ subscribe architecture which is similar to that of MQTT
- The difference is that the broker is divided into two main components: exchange and queues
- The exchange is responsible for receiving publisher messages and distributing them to queues based on predefined roles and conditions
- Queues basically represent the topics and subscribed by subscribers which will get the sensory data whenever they are available in the queue

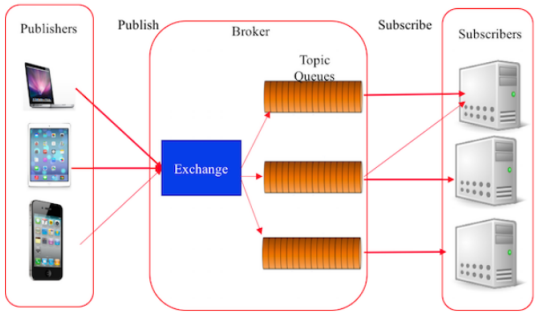

Figure 6. AMQP

C. CoAP

- Constrained Application Protocol
- CoAP enables low powered devices to use REST services

- It is built on UDP alongwith a lightweight reliability mechanism
- Two sublayers: **Messaging** and **Request/Response**
- Messaging layer is responsible for reliability and duplication of message
- Request/Response layer is responsible for communication
- Four messaging modes:
  - Confirmable: Reliable transmission
  - Non-confirmable: Unreliable transmission

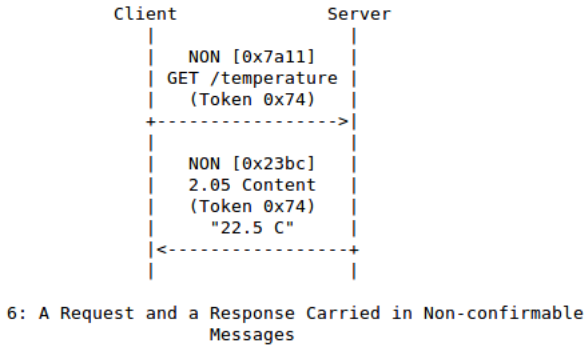

Figure 7. Non-Confirmable transmission

  - Piggyback: Response message is piggybacked alongwith acknowledgement

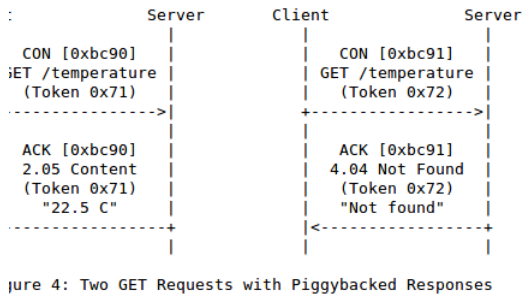

Figure 8. Confirmable Piggybacking

  - Separate: Response message is separate from acknowledgement

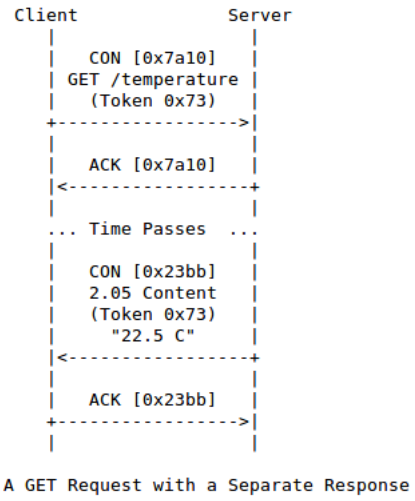

Figure 9. Confirmable Separate

- Reliability is provided by marking a message as Confirmable (CON).
- A Confirmable message is retransmitted using a default timeout and retransmissions, until the recipient sends an Acknowledgement message (ACK) with the same Message ID from the corresponding endpoint
- A message that does not require reliable transmission can be sent as a Non-confirmable message (NON). These are not acknowledged, but still have a Message ID for duplicate detection
- When a recipient is not able to process a message, it may reply with a Reset message (RST).