Wireless Media Access Issues in Internet of Things

When it comes to communication using a wireless medium there is always a concern about the interference due to other present wireless communication technologies. Wireless means communication and message transfer without the use of physical medium i.e., wires.

Let us understand how communication is done between them. Different Mobile stations(MS) are attached to a transmitter/receiver which communicates via a shared channel by other nodes. In this type of communication, it makes it difficult for the MAC design rather than the wireline networks.

The very important issues which are observed are: Half Duplex operation, Time-varying channel, and Burst channel errors.
These are explained as following below.

1. Half Duplex operation:
Half-duplex transmission means when the sender and receiver both are capable of sharing data but one at a time. In wireless transmission, it is difficult to receive data when the transmitter is sending the data because during transmission a large amount or a large fraction of signal energy is leaked while broadcasting. The magnitude of the transferred signal and received signal differs a lot. Due to which collision detection is even not possible by the sender as the intensity of the transferred signal is large than the received one. Hence this causes the problem of collision and the prime focus should be to minimize the collision
2. Time-varying channel :
Time-varying channels include the three mechanisms for radio signal propagations they are Reflection, Diffraction, and Scattering.

- **Reflection –**
  This occurs when a propagating wave carrying information intrudes on an object that has very large dimensions than the wavelength of the wave.
- **Diffraction –**
  This occurs when the radio path between the transmitter and the receiver is collided by the surface with sharp edges. This is a phenomenon which causes the diffraction of the wave from the targeted position.
- **Scattering –**
  This occurs when the medium through from the wave is traveling consists of some objects which have dimensions smaller than the wavelength of the wave.

While transmitting the signal by the node these are time shifted and this is called multipath propagation. While when this node signals intensity is dropped below a threshold value, then this is termed as fade. As a result Handshaking strategy is widely used so as a healthy communication can be set up.

3. Burst channel errors :
Burst channel errors are called as a contiguous sequence of symbols, which are received in a communication channel, in which the first and last symbols has an error and there is no evidence of contiguous sub-sequence of corrected received symbols. When time-varying channels are used then signals strengths are introduced due to which errors are observed in transmission. For these channels in wireline networks, the Bit rate is high as 10^{-3}.

Routing Protocols

Routing is a process in which the layer 3 devices (either router or layer 3 switches) find the optimal path to deliver a packet from one network to another. Dynamic routing protocols use metric, cost, and hop count to identify the best path from the path available for the destination network. There are mainly 3 different classes of routing protocols:

1. Distance Vector Routing Protocol :
These protocols select the best path on the basis of hop counts to reach a destination network in a particular direction. Dynamic protocol like RIP is an example of a distance vector routing protocol. Hop count is each router that occurs in between the source and the destination network. The path with the least hop count will be chosen as the best path.
Features –

- Updates of the network are exchanged periodically.
- Updates (routing information) is not broadcasted but shared to neighbouring nodes only.
- Full routing tables are not sent in updates but only distance vector is shared.
- Routers always trust routing information received from neighbor routers. This is also known as routing on rumors.

Disadvantages –

- As the routing information is exchanged periodically, unnecessary traffic is generated which consumes available bandwidth.
- As full routing tables are exchanged, therefore it has security issues. If an **un-authorized** person enters the network, then the whole topology will be very easy to understand.

- Also, the broadcasting of the network periodically creates unnecessary traffic.

2. Link State Routing Protocol :
These protocols know more about Internetwork than any other distance vector routing protocol. These are also known as SPF (Shortest Path First) protocol. OSPF is an example of link-state routing protocol.
Features –

- Hello, messages, also known as keep-alive messages are used for neighbor discovery and recovery.
- Concept of triggered updates is used i.e updates are triggered only when there is a topology change.
- Only that many updates are exchanged which is requested by the neighbor router.

Link state routing protocol maintains three tables namely:

1. **Neighbor table-** the table which contains information about the neighbors of the router only, i.e, to which adjacency has been formed.
2. **Topology table-** This table contains information about the whole topology i.e contains both best and backup routes to a particular advertised networks.
3. **Routing table-** This table contains all the best routes to the advertised network.

Advantages –

- As it maintains separate tables for both the best route and the backup routes (whole topology) therefore it has more knowledge of the internetwork than any other distance vector routing protocol.
- Concept of triggered updates is used therefore no more unnecessary bandwidth consumption is seen like in distance vector routing protocol.
- Partial updates are triggered when there is a topology change, not a full update like distance vector routing protocol where the whole routing table is exchanged.

3. Advanced Distance vector routing protocol :
It is also known as hybrid routing protocol which uses the concept of both distance vector and link-state routing protocol. Enhanced Interior Gateway Routing Protocol (EIGRP) is an example of this class of routing protocol. EIGRP acts as a link-state routing protocol as it uses the concept of Hello protocol for neighbor discovery and forming an adjacency. Also, partial updates are triggered when a change occurs. EIGRP acts as a distance-vector routing protocol as it learned routes from directly connected neighbors.

REST vs. SOAP

REST and SOAP are 2 different approaches to online data transmission. Specifically, both define how to build application programming interfaces (APIs), which allow data to be communicated between web applications. Representational state transfer (REST) is a set of architectural principles. Simple object access protocol (SOAP) is an official protocol maintained by the World Wide Web Consortium (W3C). The main difference is that SOAP is a protocol while REST is not. Typically, an API will adhere to either REST or SOAP, depending on the use case and preferences of the developer.

REST: representational state transfer

REST is a set of architectural principles attuned to the needs of lightweight web services and mobile applications. Because it's a set of guidelines, it leaves the implementation of these recommendations to developers.

When a request for data is sent to a REST API, it’s usually done through hypertext transfer protocol (commonly referred to as HTTP). Once a request is received, APIs designed for REST (called RESTful APIs or RESTful web services) can return messages in a variety of formats: HTML, XML, plain text, and JSON. JSON (JavaScript object notation) is favored as a message format because it can be read by any programming language (despite the name), is human- and machine-readable, and is lightweight. In this way, RESTful APIs are more flexible and can be easier to set up.

An application is said to be RESTful if it follows 6 architectural guidelines. A RESTful application must have:

1. A client-server architecture composed of clients, servers, and resources.
2. Stateless client-server communication, meaning no client content is stored on the server between requests. Information about the session’s state is instead held with the client.
3. Cacheable data to eliminate the need for some client-server interactions.
4. A uniform interface between components so that information is transferred in a standardized form instead of specific to an application’s needs. This is described by Roy Fielding, the originator of REST, as “the central feature that distinguishes the REST architectural style from other network-based styles.”

5. A layered system constraint, where client-server interactions can be mediated by hierarchical layers.
6. Code on demand, allowing servers to extend the functionality of a client by transferring executable code (though also reducing visibility, making this an optional guideline).

SOAP: simple object access protocol

SOAP is a standard protocol that was first designed so that applications built with different languages and on different platforms could communicate. Because it is a protocol, it imposes built-in rules that increase its complexity and overhead, which can lead to longer page load times. However, these standards also offer built-in compliances that can make it preferable for enterprise scenarios. The built-in compliance standards include security, atomicity, consistency, isolation, and durability (ACID), which is a set of properties for ensuring reliable database transactions.

Common web service specifications include:

- **Web services security (WS-security)**: Standardizes how messages are secured and transferred through unique identifiers called tokens.
- **WS-Reliable Messaging**: Standardizes error handling between messages transferred across unreliable IT infrastructure.
- **Web services addressing (WS-addressing)**: Packages routing information as metadata within SOAP headers, instead of maintaining such information deeper within the network.
- **Web services description language (WSDL)**: Describes what a web service does, and where that service begins and ends.

When a request for data is sent to a SOAP API, it can be handled through any of the application layer protocols: HTTP (for web browsers), SMTP (for email), TCP, and others. However, once a request is received, return SOAP messages must be returned as XML documents—a markup language that is both human- and machine-readable. A completed request to a SOAP API is not cacheable by a browser, so it cannot be accessed later without resending to the API.

SOAP vs. REST

Many legacy systems may still adhere to SOAP, while REST came later and is often viewed as a faster alternative in web-based scenarios. REST is a set of guidelines that offers flexible implementation, whereas SOAP is a protocol with specific requirements like XML messaging.

REST APIs are lightweight, making them ideal for newer contexts like the Internet of Things (IoT), mobile application development, and serverless computing. SOAP web services offer built-in security and transaction compliance that align with many enterprise needs, but that also makes them heavier. Additionally, many public APIs, like the Google Maps API, follow the REST guidelines.