CHAPTER 4

Module IV

Wireless Sensor Networks

Syllabus :

History and context, Node, Connecting nodes, Networking nodes, Securing communication, Standards and Fora, Networking and the Internet -IP Addressing, Protocols - MQTT, CoAP, REST Transferring data.

4.1 Introduction to Wireless Sensor Network

- Wireless Sensor Network senses and gathers together data using sensors distributed spatially in the geographical region and collects it to a centralized location with the help of wired, wireless or sometimes hybrid network for processing.
- Usually WSN is used to detect physical and environmental changes like temperature, pressure, motion, heat etc.
- WSN focuses on sensing and gathering data and routing it for further processing.
- The motive behind vast development in WSN was military and battlefield surveillance.
- WSN has multiple nodes ranging from few hundreds to thousands in number scattered throughout vast geographical region.
- Each of these nodes at least has a sensor attached to it obviously for the sensing purpose. Sometimes a single node has multiple sensors attached to it (temperature, pressure, motion, etc.).
- A node has an electronic circuit interface for the sensors inside, a microcontroller, a radio transceiver with antenna and battery as energy source.
- These node senses data and has a routing capability.
- This data is processed and provided to the end user in upper layers as shown in Fig. 4.1.1.
- Sensor nodes are usually connected to base station of sink that communicate between nodes and users.
- Intelligent logic can be provided here for processing or computing the data gathered by nodes.
- The processed data is converted into user representable information and provided to the end user via Internet connectivity.
- Routing protocols used in WSN are distributed and reactive which means nodes look for a route to transfer data only when some data is gathered or intermediate nodes have some data to be transmitted.

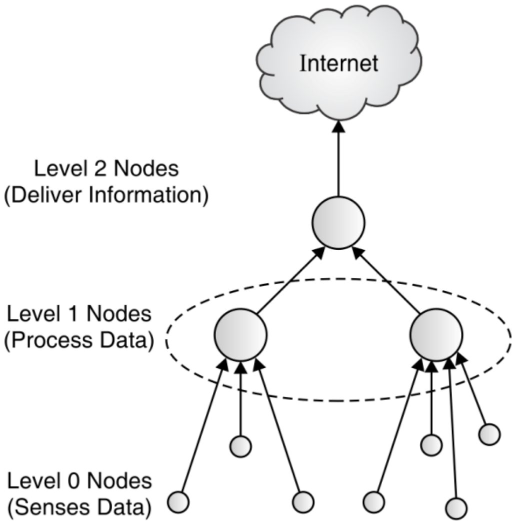


Fig. 4.1.1 : Simple WSN architecture

- Ad hoc On demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are used popularly for routing.
- The topology of WSN can be a simple star topology or multihop mesh network.
- The lifespan of a WSN depends upon the energy source of nodes as nodes are distributed over a large geographical area. So the algorithms and protocols used in WSN must be fault tolerant and robust to increase the lifespan of the node.
- Mobile Sensor Network (MSN) is a WSN in which nodes are mobile and can change location based on their own or due to environmental changes.
- The main difference between static WSN and MSN is the data routing mechanism.
- In static WSN the route is mostly predictable as the nodes in the system hardly changes but in MSN the number of nodes in the network at given point of time may not be the same later.
- Based on the number of nodes and their types the routing mechanism and routes can change.
- The development in WSN has led to the inception of WSAN i.e. wireless sensor and actuators network, which is capable of sensing environmental changes, processing this data and making decisions based on observations and performing appropriate actions.
- WSAN are used in battlefield surveillance, biological and chemical haphazard detection, climate control systems, nuclear power plants etc.
- Along with WSAN, one more extended version of WSN is becoming famous which is USN i.e. Ubiquitous Sensor Network.
- USN is considered as a network of smart devices/sensors which will become universal / global one day.

Examples of WSN

1. Forest fire detection
2. Weather monitoring systems
3. Manufacturing process control system in large industries
4. Hurricane, avalanche detection systems
5. Military surveillance etc.

4.2 History and Context

- Wireless sensor networks in its evolution is equally contributed by scientists, researchers and the intellectual commercial leaders of field.
- With the need of sensing, computation and communication in top level projects like smart dust in late 90's, WSN becomes a necessity.
- Size, power and cost were the key area of focus at that time. WSN promises to address all these factors very efficiently.
- There were many conferences, interesting academic presentation (workshops) where the use and application area wireless sensor network are demonstrated very innovatively.
- The main motivation was to put low cost sensor anywhere and the efficient communication can be achieved without wires.
- Soon the diverse fields shown the interest and started incorporating WSN in their application areas like Light control, Access Control, Home automation, Heating Ventilation Air Conditioning (HVAC), smart transportation etc.
- With increasing use and demand of WSN, IEEE came up with first version of IEEE 802.15.4 in 2003. This addresses both MAC and physical layer.

4.3 Node

- The node or WSN's wireless mote is tiny intelligent unit containing few integrated circuits. These may be powered by battery.
- More sophisticated motes can opt for alternate sources of power like day light.
- Central to the mote is the most intelligent chip called to microcontroller where all the tiny peripherals and other secondary chips got connected. This acts as the tiny processor within the mote.
- This intelligent piece of processor or the microcontroller controls the sampling of communication and radio chip.
- Microcontroller sends the signal to radio chip which in turn sends it to the antenna of mote.
- Dedicated sensor chips in mote are responsible for sensing the digital or analog data based on the type of application capability of sensing chip.

4.4 Connecting Nodes

- Radio frequency is the most basic widely used methodology for connecting nodes.
- Transmitter does not sends constant wave signal, instead to transfer information some aspects of wave is intentionally changed. This is called the modulation.
- ON-OFF keying is simple mechanism where the tone is turned on and off to convey the information.
- In some form of communication, the tone is not entirely turned off, instead amplitude is changes. This is called ASK (Amplitude Shift Keying).
- In other case the transmitter modulates the frequency. This is called FSK (Frequency Shift Keying).

- Another is PSK (Phase Shift Keying) where the where signal is transferred by modulating the phase of carrier.
- Interference or the unwanted components received by the antenna. Sensitivity of radio can be defined as the amount of power required to achieve the specific bit error rate. This depends upon the amount of noise present and on the signal to noise ratio.
- Ensuring the reliability in successful connection and communication of wireless nodes is one of the key challenging area of wireless sensor network.

4.5 Networking Nodes

- Encapsulation of many components inside the mote is required to make it successfully communicate over the network.
- Making the mote available on a network and making it available over multiple hops, has many inherent challenges.
- The firmware or software inside the mote has to decide on the protocol, timing, frequency etc. of communication.
- Complex but small codes are needed to run inside the mote. These are mostly exist in the form of firmware. Once written, it runs for life time. More sophisticated motes however has provision of firmware updates.
- Layers of communication plays an important role making the available and serviceable over the network.
- The most important layer for the motes is Media Access Control layer. It control the state of WSN chip. It includes duty cycle and energy aspects of node. It also has to address changing topology of wireless sensor network.
- More sophisticated WSN MAC has the provision of switching off the motes in inactive hours. MAC is designed for power supply co-ordination. Power is supplied only when the communication needs to happen. These are energy efficient MAC protocol.
- Preamble sampling protocols also contributes in successfully operating and networking nodes. It has the feature of listening for very short time to sense the ongoing transmission. CI (Check interval) is the term used to define duration of time the mote waits between two transmissions.
- Apart of it, framed MAC protocol is also there which formulates a schedule that all other nodes follow for transmission. This saves energy but required greater intelligence for co-ordination.

4.6 Problems in Securing Communication Standards Fora

- In standard IEEE 802.15.4 and ZigBee Alliance protocols, when the Rx receives the message (MSG), it verifies its validity (integrity, authenticity and freshness). If the message is valid, then the Rx sends an unprotected ACK to the Tx, which considers the communication successfully concluded upon its receipt, with no check upon the ACK authenticity (i.e., its coming from the expected Rx node) and freshness (i.e., its being a new ACK, and not an old ACK copied and repeated by a non authorized node).
- The lack of authentication and freshness verification on the ACK could seriously threaten the security of the whole network. For instance, let us consider the simple case of an attacker trying to avoid that a message arrives to the Rx, thus starting a MITM attack. It can first simply send an interference noise to the Rx at the same time as the Tx, thus preventing the Rx from properly receiving the MSG sent by Tx.

- Afterwards, the attacker can send a fake ACK to the Tx. This way, since the ACK is not protected, the Tx can be fooled that Rx successfully received the MSG.
- Another limit of standard protocols is that they verify the MSG freshness by checking a sequence number provided by a simple counter. They are consequently prone to DoS-like attacks.
- An attack can be carried out by assembling a fake message that is compliant with the protocol format and by setting its sequence number equal to the maximum counting value. This way, the counter of the node receiving such a fake message will overflow. This will make the counters of the Tx and Rx no longer synchronous, so that the Rx will discard all following messages from Tx.

4.6.1 Solution for Securing Communication Standards

- Consider the case of a master/slave network with one master node, acting also as network manager, and several slave nodes. The protocol can be applied to any kind of WPAN by means of straightforward modifications.
- Similarly to the standard IEEE 802.15.4 and ZigBee protocols, our protocol guarantees authentication and integrity of the MSG by means of a Message Authentication Code (MAC), that is generated by encrypting the message in clear text by an AES algorithm. Moreover, differently from the standard IEEE 802.15.4 and ZigBee protocols, our protocol: i) Guarantees the authenticity and freshness of the ACK, thus avoiding MITM attacks; ii) Provides a new mechanism to guarantee the freshness of the MSG, that is able to protect the WPAN with respect to DoS-like attacks.
- To guarantee the authenticity of the ACK, we propose to generate a MAC for the ACK, by encrypting the ACK in clear text by an AES algorithm. To guarantee the freshness of the ACK and the MSG, as described in more details later in this section, our protocol embeds a rolling code sequence (#seq) on both the ACK and MSG, and provides a original mechanism to synchronize the Tx and Rx, that makes the WPAN immune to DoS-like attacks. The general structure of the derived MSG or ACK is schematically shown in Fig. 4.6.1.

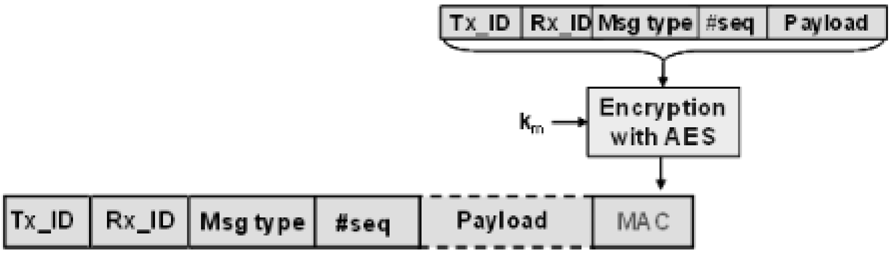


Fig. 4.6.1 : Structure of a MAC or ACK of protocol.

- The fields Tx_ID and Rx_ID contain the identification codes (IDs) of the transmitter Tx and receiver Rx, respectively. The Payload is the useful part of the message, containing data, commands or ACKs. The field Msg_type indicates the type of message (e.g., command, data, ACK, synchronization, etc.) included in the payload field. The field #seq contains the current sequence number of the rolling code of the node (Tx/Rx) sending the message. Finally, the MAC of the MSG or ACK is generated by encrypting the first part of the message (i.e., Tx_ID, Rx_ID, Msg_type, #seq and Payload) by the AES algorithm and a secret key km.
- As can be seen from Fig. 4.6.1, the useful message (i.e., the whole message, but for the MAC) is sent in clear text. This allows to identify the Rx of the message and to verify the correctness of #seq without any decryption, thus reducing power consumption and the impact on communication latency. Of course, this approach can not be used if the message carries critical data, while it does not give rise to any security flow if the message consists of a simple command, as it is usually the case in WPANs.

4.7 Networking and Internet IP Addressing

IP is the standard communication protocol in the Internet. Several attempts have been made to port the TCP/IP to Wireless Sensor Networks, because it would ease data acquisition from external applications. This would make it possible to integrate applications more easily into existing networks. On the other hand, IP was initially designed for non resource constraint systems. This causes a significant decrease in bandwidth mostly because of its large header data.

4.7.1 6LoWPAN

- 6LoWPAN communication protocol represents the communication done via IPv6 over Low power Personal Area Network.
- 6LoWPAN is a network layer protocol.
- 6LoWPAN is designed for lower powered devices where communication overhead should be less.
- Devices with low processing and communication capabilities use this protocol in network layer.
- 6LoWPAN works over frequency range of 2.4GHz and has data transfer rate of 250 Kb/S.
- 6LoWPAN in network layer and 802.15.4 in link layer works together and describes compression mechanism for IPv6 packets for communication in LR-WPAN.
- 6LoWPAN encapsulates IPv6 long headers in IEEE802.15.4 small packets and are not allowed to exceed 128 bytes.
- 6LoWPAN specification provides following core features:

  Different address length, low bandwidth, low cost, power consumption, different topologies including star or mesh, mobility, scalable networks, long sleep time and unreliability.

6LoWAPN has to tackle following key issues to make it as a low powered protocol

- **Header compression :** LoWPAN is supposed to be consuming less power, but having larger packet size leads to loss of energy. IPv6 header requires 40 bytes of storage so compression mechanism is must to save energy with IPv6 and LoWPAN (6 LoWPAN).
- **Packet fragmentation and reassembly :** Packet transmission in a network consumes energy, larger the packets size higher the energy requirement. So making the packet size was needed and low packet size also reduces the chances of packet loss especially during the use of lossy network like 802.15.4.
- Reworking of neighbour discovery defined in RFC4861 and 4862 so as to meet low power requirement.
- Availability of mesh-under routing done by 6LoWPAN Adaptation Layer.

6LoWPAN currently defines following headers

  - The Mesh Addressing Header
  - Hop by Hop Processing Header
  - Destination Processing Header (Example fragment Header)
  - Payload transport Header (Example IPv6 and UDP compression Header)
- The First byte of each header identifies the type of header, is called as the dispatch byte.

- Along with above explained types additional types can be added to 6LoWPAN and space is available in dispatch byte for future development.

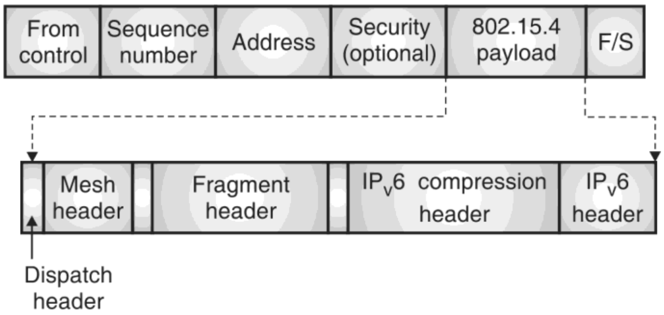


Fig. 4.7.1 : 6LoWPAN header with dispatch byte

- As shown in Fig. 4.7.1 above each header starts with a dispatch byte which represents which type of header is going to be used.

Byte contents	Header Type
00	Not 6LoWPAN
01	IPv6 Compression Header
10	Mesh Header
11	Fragmentation Header

Mesh header

In mesh under routing done in 802.15.4, Source and Destination Address of each hop needs to be specified in 802.15.4 MAC Frame. Mesh Header provides a container to keep original and final 802.15.4 addresses.

IPv6 compression header

IPv6 compression is necessary in 6LoWPAN to reduce the energy consumption associated with original IPv6 Header.

Various methods are implemented in this approach

- Creating an IPv6 Unicast address from EUI64 802.15.4 address in which a standard 64 bit address in converted into 16 bit short address.
- *HC1* (Header Compression 1) compression format for IPv6 header and *HC2* (Header Compression 2) compression format for UDP header were available but are now replaced by *New HC* compression format for IPv6 header and NHC (Next Header Compression).
- A recent approach is Context Based Compression called IPHC in which selective compression of IPv6 flow labels.
- IPHC sends compressed IPv6 fields, uncompressed IPv6 fields NHC Header in sequence.

Fragmentation header

- The first fragment defines fully reassembled packet size and tags for datagram common to an IP packet.
- This can be used by the receiver to identify fragments belonging to the same packets.
- Following to the first fragment, rest of the fragments describe the offset of the next fragment in the full IP Packet.
- Protocols - MQTT, CoAP, REST Transferring data.

4.8 MQTT

- MQTT stands for Message Queue Telemetry Transport is a famously used IoT protocol is an Application Layer protocol.
- MQTT was first developed and deployed by IBM but few years back IBM made it Open Source for better development of the protocol.
- MQTT uses publish subscribe model of communication as seen in earlier chapter. The broker of the publish subscribe model handles the queues which manages the topics.
- In MQTT client server communication, client connects to the server and publishes messages to topics available on the server.
- Intermediate broker manages these messages from clients and forwards it to the consumers subscribed to the topics.
- MQTT is specially intended for resource-constrained devices having low power, low bandwidth and network with high latency like dial-up lines and satellite links.

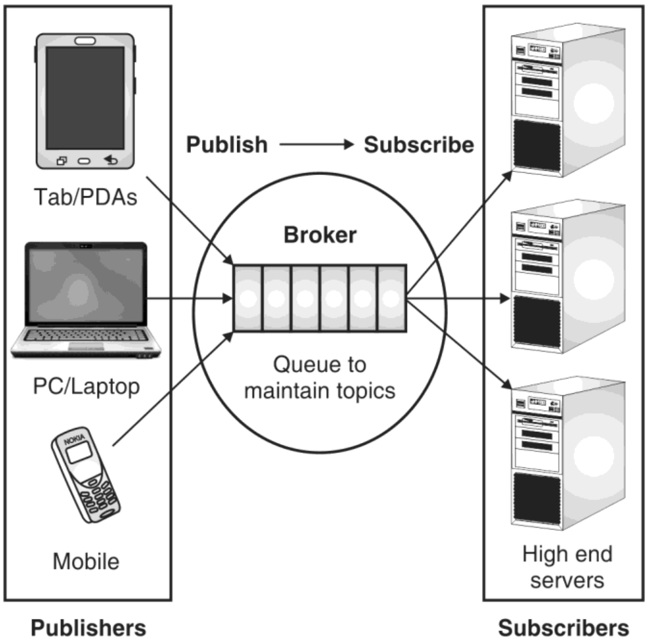


Fig. 4.8.1 : MQTT architecture

- MQTT is useful in applications and devices where resources (processing and memory) are limited and has low bandwidth.
- Because of this MQTT has a low power footprint which makes it suitable for IoT application development.
- The main aim of MQTT is to collect data from many devices; sensors distributed in the network and transport that data to the IT industries for further processing.
- This goal needs to be done in telemetry fashion i.e. remotely with minimal human intervention.
- MQTT based broker can engage thousands of device connection and that too concurrently.
- MQTT works on top of TCP, which maintains the reliability of messages and no data loss is there.
- MQTT is also helpful in connecting computational devices like Arduino, Raspberry Pi, BBB to the web services.
- Facebook uses MQTT as an integral part of FB mobile applications due to the low power requirements and it is very light on network bandwidth.
- MQTT has been assigned port number 1883 without SSL and 8883 for MQTT with SSL.

- MQTT is ideal for huge network of small devices and sensors that need to be monitored or controlled via a back-end server from the Internet.

4.9 CoAP

- CoAP stands for Constrained Application Protocol, invented by IETF for RESTful environment, which is an Application Layer protocol used by IoT applications.
- CoAP can be considered smaller version of SoAP specifically designed for low powered devices used in IoT applications.
- CoAP used for machine to machine (M2M) communication where the applications are meant for small embedded devices, controlled environment and constrained networks.
- Similar to HTTP, CoAP is also a web transfer protocol and follows request-response model.
- CoAP uses client server communication using UDP based communication by default and occasionally with TCP.
- CoAP works with HTTP to provide the basic support of the web. In this way proxies can be used to access the CoAP resources via HTTP in a uniform way.
- Similar to HTTP, CoAP also provides commands like GET, PUT, POST, DELETE etc. and both are simply interoperable.
- CoAP works in two main modules: Request Response Module and Messaging Module.
- Request Response Module manages the communication channel while Messaging module manages the duplication and reliability of messages in the communication.
- CoAP has four types of messaging modes :

1. Confirmable
2. Non-Confirmable
3. Piggyback
4. Separate

1. Confirmable

- This type of messages defines reliable communication and message passing.
- For each connection message Acknowledgement is received making sure that the message has received at the receivers end.

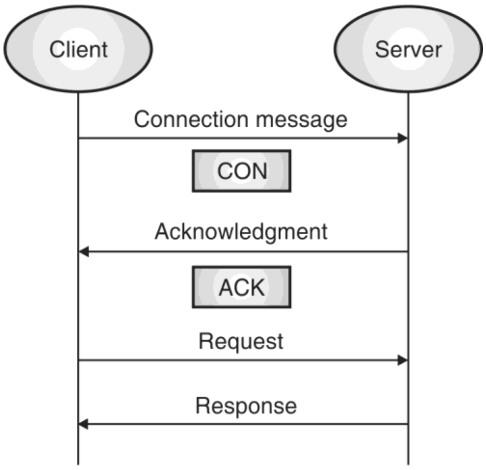


Fig. 4.9.1 : Confirmable messages

2. Non-confirmable

- This type of messages provides unreliable communication as there is no ACK on message passing hence message reception is not assured.
- So this kind of messaging is used when the loss of packets or messages is sustainable.

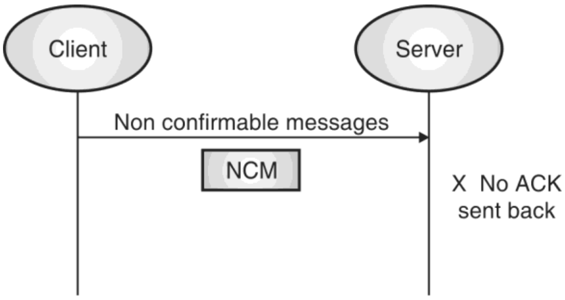


Fig. 4.9.2. : Non confirmable messages

3. Piggyback

- This mechanism is advanced confirmable messages and is used in request response model.
- When a query/request is sent to the server in client server communication, server sends the response to the query within the acknowledgement message itself.
- The ACK message itself contains the response as well.

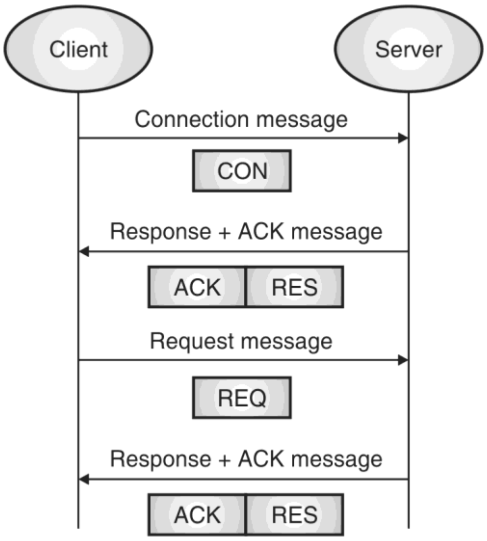


Fig. 4.9.3 : Piggyback mode

4. Separate

- In this mode the ACK messages and the Response messages are sent separately.
- When a query/request is sent to the server in client server communication, On reception of connection message server sends the ACK first making sure Request is received and ACK is sent first the response to the query is sent after the acknowledgement message.
- Response might be delayed by the server.

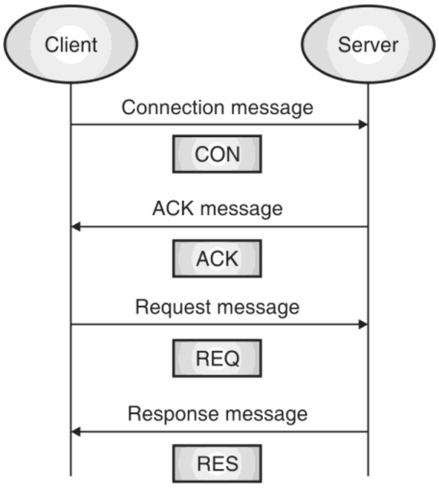


Fig. 4.9.4 : Separate mode

CoAP features in brief

1. Constrained web protocol meets M2M application requirements.
2. Works on UDP (by default) with optional support for reliability, and also has unicast and multicast requests.
3. Message exchanges : Asynchronous
4. Header overhead is low.
5. URI and content-type support;
6. Simple proxy support provides network traffic limiting, improved performance, access to the resources even if they are sleeping and of course security to some extent.
7. Also has caching capabilities.
8. CoAP works with HTTP to provide the basic support of the web. In this way proxies can be used to access the CoAP resources via HTTP in a uniform way.

4.10 REST

– Representational State Transfer which is referred as REST based API which provides a stateless communication. Let's discuss this in details.

  o REST is a set of architecture style used for designing network applications, web services or web APIs that are targets how server resources are addressed and transferred.

  o REST follows request – response type of communication model.

  o Most of the REST API works over HTTP by using the delivery methods that HTTP offers (GET, PUT, POST, DELETE etc.).

  o REST based API follows following characteristics or constraints

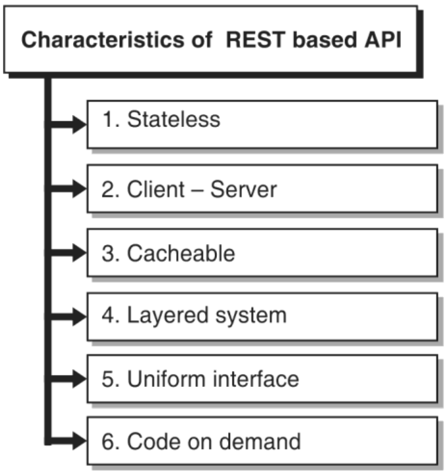
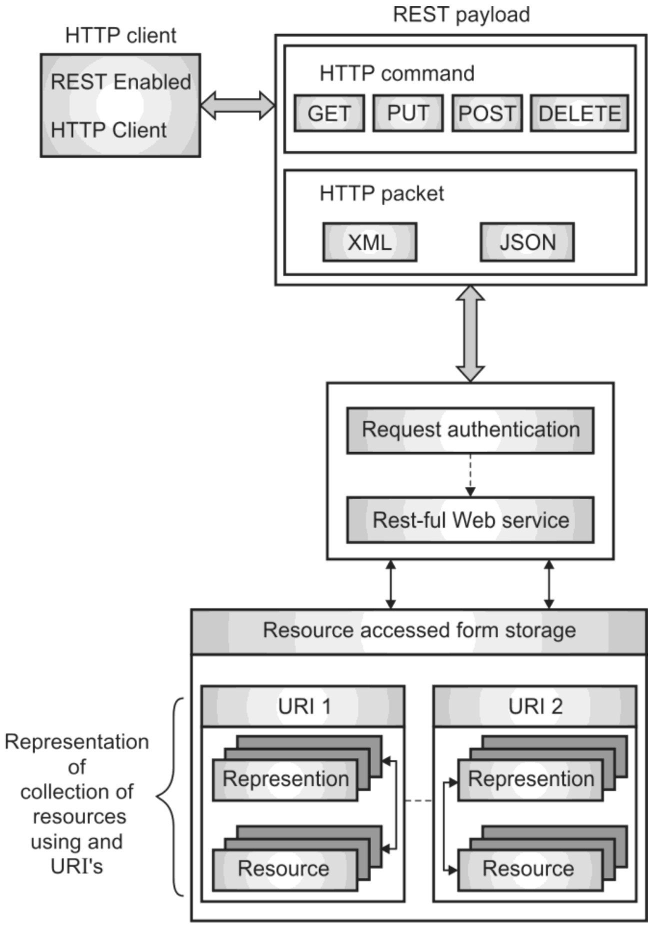


Fig. 4.10.1 : Characteristics of REST based API

1. **Stateless**

   - In REST communication each request receives its own response and it is not related with any other request or reply.
   - Because of this, each request must clearly describe its requirement and specify it in the request itself as no data from the previous context is available in communication.



Client server communication with REST APIs

Fig. 4.10.2 : REST communication flow

2. **Client – Server**

   - Client server communication distinguishes works of each side and separates it clearly.
   - As Client side will not be bothered about storage and other server work and server side will not be bothered about GUI development for the user and front end i.e. the client’s work.

3. **Cacheable**

   - Cache property defines whether the response for any request can be cached or not. If cache feature is ON then data in the response is cached in client and is readily available for reuse for next requests.
   - The request needs to be implicitly or explicitly labelled as cacheable or non-cacheable.

4. **Layered system**

   - Layered system defines the boundaries of the components within each specific layer only.
   - For example a client as a component cannot tell whether it is connected to the end server or an intermediate node/server.

5. **Uniform interface**

   - This constraint specifies that the method of communication between client and server should be uniform throughout the communication.
   - For example resources are identified by URIs in web based systems, which is uniform.
   - The data returned by the server to the client has different format and is well understood by client.

6. **Code on demand**

   - This constraint provides the server facility of sending executable codes and/or scripts to the client. Although this constraint is optional and all the other are compulsory.
   - A RESTful web service is an API implemented as a combination of HTTP and REST characteristics defined above.
   - Fig. 4.10.2 shows client server communication using REST API and Fig. 4.10.3 shows request – response model using REST.
   - As shown in Fig. 4.10.3, URIs are used to represent resources in a RESTful web service.
   - Client tries to access these resources via URIs using commands like PUT, GET, POST, DELETE etc. defined by HTTP.
   - In response to the request in RESTful web service, server responds with JSON object or XML file.

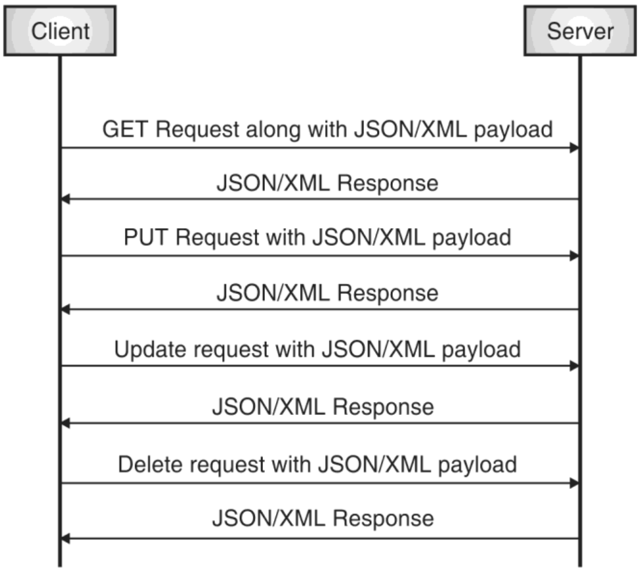

Client
Server
GET Request along with JSON/XML payload
JSON/XML Response
PUT Request with JSON/XML payload
JSON/XML Response
Update request with JSON/XML payload
JSON/XML Response
Delete request with JSON/XML payload
JSON/XML Response

Fig. 4.10.3 : Client server communication using REST

❑❑❑