Domande di IoT

1. **A LoRaWAN is deployed in a noisy environment (high interference in the background). Discuss advantages and disadvantages in the SF assignment.**
   A low spreading factor brings faster transmission since the symbols are spread on more chips (2^SF chips = 1 symbol). A higher SF on the other hand makes the transmission more robust to interference, as sensitivity decreases. Since the SNR is inversely proportional to the SF, in a noisy environment a High SF should be preferred.
2. **Briefly describe the network topologies standardized in ZigBee specifications**
   There are 3 main standardized network topologies. The star topology, where there is not direct communication between single devices, it happens only through the coordinator, that's connected to all devices. Mesh topology, whew FFD can be connected to one another, and to the coordinator. Finally, there is also the Cluster Tree Topology, that can be described as a "star of stars": nodes are organized in layers, starting from the PANC. Each router can have its own set of children end devices and routers. Devices in the same level are not connected to one another.
3. **Briefly explain how the DODAG creation process in RPL.**
   During the DODAG creation, three different messages are built: DODAG information object (DIO), used to build the DODAG and it contains information about constraints and metrics; Destination Advertisement Object (DAO), used to propagate information on destination, and the DODAG Information Solicitation (DIS), that solicits DIOs. When a node receives a DIO, it chooses if to join the graph and the node to elect as parent, deciding based on an objective function that has metrics and constraints as parameters. Once it joins the graph, the node has a route towards the root, an indication of the cost to reach the parent (according to the OF), and a rank within the graph, which is an indication of the closeness to the root of the node. If the node is a router, it advertises the graph information to children through usage of DIOs, and this continues until no more DIOs are broadcasted. In this way every node has a path to the root of the DODAG. Multiple OFs can be used, so there are more network topologies active at the same time.
4. **Briefly explain the use of DAO messages in RPL.**
   Destination Advertisement Object are used in RPL to propagate information about the destination towards the root of the DODAG. When a node joins the graph, it sends towards a parent a DAO, advertising itself as a possible destination. The parent adds the node sending this information to its router table, and the DAO is propagated upwards. DAOs are used to create downwards routes, supporting ptp and ptmp communications.
5. **Briefly explain the use of DIO messages in RPL.**
   The DODAG Information Object carries information that allows a node to discover an RPL istance, learn its configuration parameters, join the DODAG by selecting a parent and maintain it. It contains the informations used to define the objective function (metrics and constraints). It is sent from the root to the graph, and a node that receives it then advertises the graph information to its children forwarding the DIO it received.
6. **Briefly explain the use of DIS messages in RPL.**
   The DODAG Information Solicitations are object used by nodes with the purpose of discovering close-by networks and solicit the sending of a DIO in response.
7. **Describe the structure and the usage of the Routing Table and the Routing Discovery Table in ZigBee AODV routing**
   The routing table is used to store information about the best route to choose to reach a defined node; it is the result of the Ad-hoc On Demand Vector Route Discovery procedure, which instead uses the RDT to store temporary and in progress information about the route to be discovered. The RT stores for every destination, the ID of the destination itself, the next hop address, the entry

status (either active, inactive or in discovery).

The RDT has instead the following fields: ID of the route discovery (RREQ ID), source address of the RREQ, sender address of the most recent lowest cost RREQ, the forward cost (the cost accumulated until the current device), and the residual cost (accumulated path cost from the current devide to the destination).

A RREQ message is broadcasted to neighbors by the source node that needs to send packets to the destination node. RREQ messages are flooded by receiving nodes. When a node re-broadcasts a RREQ, it sends up a reverse path towards the source with an accumulated cost and the previous hop; RREQs with an accumulated cost than the one that's stored are dropped, otherwise the path is updated. When the intended destination receives a RREQ, it sends an RREP that goes back on the path of the RREQ to the sender previously stored. During the forward of the RREQ the forward cost gets calculated, and during the forwarding of RREPs the same happens for the residual cost. The residual cost calculated at the source node when it receives the last RREP is the cost of the best path.

8. **Briefly list the main adaptation functionalities introduced by the 6LowPAN standards**

   6LowPAN grants the user the capability of using IPv6 over low power wireless links. There are two main adaptation functionalities are the header compression and the fragmentation of the IPv6 packet.

9. **Briefly describe the header compression standardized in 6LowPAN**

   In order to make transmission over constrained network easier, IP and UDP headers are compressed. Information available or derivable from lower layers gets omitted (for example the length of the PDU for UDP). A Header Compression Header is used to describe the type of compression; it precedes the header of IPv6 and the UDP's one. There is no information loss. It is done by mapping values in the HCH to common values of fields of the IPv6 header, and by specifying in the HCH which information is hidden. Address compression is performed through the usage of context and exploiting whether the address is link local or not, and this helps reducing the size of the address since addresses within 6LowPAN have usually common prefixes. Traffic Class and Flow Label can be compressed in 4 different ways (selecting the information to elide), and the HOP limit field can be inline or three common values (1,64,255).

   UDP headers are compressed through the reduction of the allowed number of ports, through the omission of the length field and the omission of the checksum if other checks are used.

10. **Briefly describe the IPv6 packet fragmentation**

    IPv6 packets needs a minimum of 1280 bytes of length, whereas the standard 802.15.4 has a maximum payload of 127 bytes. So, a Fragmentation Header (FH) is used. This header includes the dimension of the fragment, the ID of the PDU the fragment belongs to, and the fragmentation offset, but is not efficient.

11. **Briefly explain the COAP Observe operation mode**

    In COAP the request is of PULL type, which means that the client requests updates with explicit requests; since data in WSN is usually produced periodically, it has to be retrieved also periodically. The Observation Mode allows clients to requests periodical updates with a single GET request. When included in a GET request, the client is added to the list of observers of a resource. When a new value of said resource is available, the server sends it back to the client in a response, without an explicit request. The observe option is set to a value that is used to sort chronologically the responses. If the client can't be added to the list of observes, the request is treated like a normal GET request. The client can ask to be either registered or unregistered, in the latter it gets removed from the observer list.

12. **Briefly explain the usage and differences between Message ID and Token fields of COAP**

    The message ID identifies a message as a communication that must be acknowledged; the Token field identifies a request for a resource, and is followed by a response. A message has the same MID of the ACK of that message; a response has the same token field of the associated request, but a different MID (if separate from the ACK of the request). The ACK of the response (if asked by CON flag) has the same MID of the response.

13. Briefly describe the Block operation mode of COAP

The Block operation mode allows to limit the payload size, the same way the 6LowPAN adaptation layer fragmentation works. When a resource representation is so big it can't be comfortably transferred in the payload of a single CoAP datagram, a Block option can be used to indicate a block-wise transfer: so the fragmentation is brought up at the application layer.

When the Block2 option is added to response messages, it means the resource has been split into blocks, and the client will make multiple requests (with the Block2 option), so it will obtain all the blocks of the resource. The option Block2 has 3 fields: incremental number of blocks requested in the response, a flag indicating there are more blocks left, and the block size.

14. Differences between CoAP and MQTT

The main difference between this two is that CoAP (except for the observe option) is a PULL paradigm, so clients ask for resources. MQTT is a PUSH publish/subscribe paradigm, in which clients can subscribe to a topic by sending a message to the MQTT broker, which will send new data on the topic to the subscribers. CoAP allows connections between nodes, meanwhile MQTT has all clients connected to a single broker. Finally, in CoAP the clients know the network topology, in MQTT only the broker oversees routing and delivering messages.

15. Briefly describe the quality of service levels of MQTT

In the QoS field we can find 3 different levels of services. Each subscription to a topic has its own requested QoS.

QoS 0, "At most once": a message is sent once without need of ACK, in a best-effort way.

QoS 1, "At least once": a message sent with this QoS needs to receive an ACK, and it gets retransmitted until and ACK comes.

QoS 2, "Exactly once": slowest and safest level. It requires two request-response patterns in a four-part handshake. This makes sure that the message will be received just once.

16. Briefly describe the utility of MQTT retain functionality

If a message gets published with this flag, the message will be stored by the broker. When a new client subscribes to this topic, it will receive the retained message as soon as it subscribes (instead of waiting for a publish from the sensor).

17. Briefly explain the use of persistent sessions in MQTT

This kind of session is used to avoid complete erasure of the status of the session when the clients disconnect. Persistent sessions allow to save in the broker the topics of a client and other data. Apart from the subscriptions, the broker saves all QoS 1 and 2 messages that didn't receive an ACK, the QoS 1 and 2 messages not received when the client was offline and the QoS 2 messages that the broker didn't acknowledge. The client saves QoS 1 and 2 messages not acknowledged by the broker and the QoS 2 messages that it did not sent an ACK for.

18. Briefly explain how the PAN coordinator assigns CFP slots to sensor nodes

The slots are assigned on a statistical basis, considering the needs of different nodes. It can be done from the minimum data rate required by nodes: if this data rate is called R, we can dimension the slot with the fraction L/R (with L being the packet length); the Beacon Interval has the duration of one slot. Then we assign the slots by dividing the highest data rate needed by a node by R and rounding: the result is the number of slots the node is assigned. The length of a slot is the product of the channel data rate and the size of the packet sent. CFP slots, once computed, are assigned through the beacon at the start of the BI by using the GTS fields in the beacon frame.

19. **A mote runs the IEEE 802.15.4 Carrier Sense Multiple Access procedure. The current parameters are CW=2, NB=1, BE= 2. Briefly explain what the use of these parameters is. In which range the mote will choose the next slot for sensing the channel?**
    BE is the backoff exponent, it determines how many backoff periods a device must wait before attempting to perform channel assessment. It is incremented by one every time the assessment is not successful. CW is the contention window, number of backoff periods a channel must be assessed as free before the node can transmit. NB is number of times the CSMA/CA algorithm was required to backoff, so the times the assessment was unsuccessful. In this case, the range for choosing the slot for sensing the channel will be in the range [0, 2^BE-1] = [0,3]
20. **Briefly describe the process of active scanning in the context of IEEE 802.15.4 network formation**
    Active scanning is used by a node to discover available networks over different channels. The node that start performing the scan sends out a command frame, a beacon request, on the first channel; available PANC answer with beacons containing information about the network and the PANC ID; then the node changes channels and repeats the procedure for all channels available. At the end it chooses a PANC ID whose network to join.
21. **Briefly describe the utility of backlog estimate procedures in RFID collision arbitration mechanisms. Sketch the guidelines of Schoute's estimate**
    Dynamic Frame ALOHA is more efficient than plain ALOHA, but to implement it we need to dimension the current frame to the size of the current backlog n (number of nodes whose transmissions collided in previous frame). Since the initial population is unknown, we have to estimate it. Under the assumption that the frame size can be equal to the current backlog, the number of terminals transmitting in a slot approximated by a Poisson process with intensity 1 terminal/slot, it can be proven that the average number of terminals in a collided slot is $H = \frac{(1-e^{-1})}{1-2e^{-1}} = 2.39$. The backlog is estimated through Schoute's estimate as: $n_{est} = round(Hc)$, with c the number of collided slots.
22. **Briefly explain the main differences between Frame ALOHA and Dynamic Frame ALOHA**
    In Frame ALOHA the size of the frame is always the same, in Dynamic Frame ALOHA the size of the frame is set to the current backlog estimate, which is 2.39*number of collided slots.
23. **Three RFID tags are arbitrated by Dynamic Frame ALOHA. Tell if the following statements are true or false**
    The higher the dimension of the first frame the higher the efficiency of the arbitration process
    False: the efficiency has its best when the first frame's size is equal to the number of tags.
    The higher the dimension of the first frame, the higher the average throughput after the first frame
    True
24. **Define all the sources of energy consumption for a sensor node in a sensor network**
    The main energy consumption sources are: energy required to power up the TX/RX circuit, energy needed to sustain a certain TX power level, energy spent during wake up of the circuit, energy spent while being idle and sleeping, energy spent for data processing and energy spent from the sensor to perform measurements.

True/False Statements

1. **The IEEE 802.15.4 MAC layer is based only on random access procedures**
   False, it accepts also scheduled access in CFP for Guaranteed Time Slots, assigned by the PANC to the nodes

2. **The Schoute's estimate provides an estimate of the total number of already resolved tags**
   False, it provides an estimate of the current backlog, which consists in the tag that collided and are not yet resolved.
3. **ZigBee cluster tree routing has higher signaling overhead than ZigBee AODV routing**
   False: ZigBee cluster tree routing is simpler, as each node knows its place in the tree, and this knowledge comes from the network associations response. There is no route riscovery process.
4. **The Expected Transmission Time (ETT) is better suited as routing metric in cases where wireless links have different data rate and/or propagation delays**
   True: ETT takes into account the channel rate and therefore the time to actually send a packet over the link
5. **The ETT metric measures the average number of transmissions to send a packet over a link**
   False: average time required to send a packet over a link (and get it ACKed)
6. **Schoute's estimate gives the collision probability in a reference slot**
   False: it gives the estimated backlog for the current frame
7. **The tag arbitration efficiency in RFID system is inversely proportional to the time to resolve all the tags in the system**
   True: it is the number of tags divided the time needed to resolve them all
8. **The Route Reply messages of AODV are sent out in unicast (at IP level)**
   True: RREQs are broadcasted, RREP is sent back only to the sender node saved in the discovery table
9. **The ETX metric measures the average time to send a packet successfully over a link**
   False: it measures the average number of transmissions required to successfully send a packet over a link
10. **The slotted ALOHA has higher collision probability than un-slotted ALOHA having fixed all the other parameters**
    False: the latter's collision probability is 1-probability of success*e^(-2G), the former's is 1-e^(-G).
11. **ZigBee routing specifications define a routing metric only based on the number of hops**
    False: ZigBee routing specification define a hint for a cost to be associated with links that can be used as a metric. The cost is based on packet reception rate.
12. **The communication provided by COAP is only best-effort**
    False: it includes also reliable unicast sending with the use of CON messages
13. **RPL is a reactive routing protocol**
    False: it is a proactive routing protocol because the network is discovered before it needs to send a packet to a destination.
14. **The backoff procedure of IEEE 802.15.4 is used after collided transmissions**
    False: if the channel is busy, the transmission does not take place. In that case the BE is doubled, and the node waits for the backoff period. CSMA/CA is used, with CA standing for collision avoidance.

Formulas

$PER = 1 - (BER)^l$ (BER bit error rate, fraction of bit not correctly received; PER packet error rate, fraction of packet not correctly received; l packet length)

Transmission Time $T = \frac{L}{R}$ (L packet length[bit], R throughput[bit/s])

Slot Time $T_{slot} = \frac{L}{R}$ (R= normal data rate)

Address assignment rule: size A(d) of the range of addresses assigned to a router node at depth d<Lm, with Lm maximum depth of the tree, Dm end-devices and Rm maximum number of routers

$$A(d) = \begin{cases} 1 + D_m + R_m, & d = L_m - 1 \\ 1 + D_m + R_m A(d+1), & 0 \le d < L_m - 1 \end{cases}$$

For the address number, routers will go before end-devices

ETX: Average number of packet transmissions to successfully transmit a packet. p packet error probability from A to B and q from B to A. $ETX = \frac{1}{[(1-p)(1-q)]}$

$ETT = ETX * RTT$

Tag arbitration efficiency: N= tag population size, Ln length of the arbitration period $\eta = \frac{N}{L_N}$

Average throughput for single frame ALOHA: $E[S] = n\left(1 - \frac{1}{r}\right)^{n-1}$ Maximum for r=n

Recursive frame length: $L_n = \frac{r + \sum_{i=1}^{n-1} P(S=i) L_{n-i}}{1 - P(S=0)}$

Beacon Interval: $BI = \frac{L}{r_{min}}$

$\boldsymbol{RTT = 2 * \frac{L}{C} = \sum T}$

Correct reception of L bit $P = (1 - BER)^L$ $ETX = \frac{1}{P}$

Acronyms

DODAG: Destination Oriented Directed Acyclic Graph
DIO: DODAG Information Object
DAO: Destination Address Object
DIS: DODAG Information Solicitation
CoAP: Constrained Application Protocol
MQTT: Message Queuing Telemetry Transport
LoRaWAN: Long Range Wide Area Network
6LoWPAN: IPv6 over Low -Power Wireless Personal Area Networks
PAN: Personal Area Network
ETX: Expected Transmission Count
ETT: Expected Transmission Time
QoS: Quality of Service
LQL: Link Quality Level
RTT: Round Trip Time
CSMA: Carrier Sensing Multiple Access. /CA Collision Avoidance and /CD Collision Detect
AODV: Ad-hoc On-Demand Vector

RREQ: Route Request
RREP: Route Reply
RPL: Routing Protocol for Low Power
ROLL: Routing Over Low Power and Lossy Networks