1. Spiegare il fenomeno dei terminali nascosti nelle reti 802.11 ed eventuali soluzioni per mitigare il problema (14/01/22)

   Nelle reti 802.11 (nome tecnico della tecnologia wifi) essendo presenti stazioni mobili (MS) a diverse distanze da un access point (AP) e dalle altre MS, può accadere che due o più stazioni siano in grado di vedere/contattare l'AP perché nel loro range, ma che tra esse ci sia una distanza sufficiente a non farle individuare a vicenda.
   In questi casi quando la MS ascolta il canale verificandone la disponibilità, non rileva le trasmissioni delle altre, nonostante ci siano, ciò porterebbe ad una trasmissione simultanea sullo stesso canale e quindi a collisione.
   Per evitare questo problema è di uso comune il 4 way handshaking, un sistema che oltre al classico "2 way" (pacchetto dati + ack) aggiunge due pacchetti ulteriori, RCS cioè Request To Send che serve a verificare se il canale sia libero e CTS cioè Clear To Send che è la risposta alla MS che "autorizza" alla trasmissione e attiva nelle altre MS un timer, fino allo scadere dello stesso non saranno in grado di inviare pacchetti perché considereranno la rete occupata pur rilevandola come libera

2. Spiegare a cosa serve e come funziona il modulo **ADR** per le reti **LoRaWAN.** (14/01/22)

   Le reti LoRaWAN hanno un tipo di modulazione basato sullo Spreading Factor (SF), cioè il tempo in cui viene trasmesso un "simbolo", questo viene fatto con una sorta di modulazione in frequenza in cui utilizziamo portanti diverse per SF diversi (solitamente gli SF sono ortogonali tra loro)
   L'ADR è il componente software del Network Server delle reti LoRaWAN che si occupa di tener traccia dei Signal to Noise Ratio (SNR) di ogni stazione, cioè capta la quantità di disturbo e la potenza con cui arrivano i pacchetti dalle singole stazioni, potendo così assegnare un SF adeguato alla "distanza" (con distanza di intende non fisicamente in metri, ma anche in caso di ostacoli) tra stazione e Gateway (GW)
   In generale, ogni stazione che si connette per la prima volta riceve come impostazione un SF12, quindi il massimo, l'ADR analizzando i pacchetti ricevuti dai GW farà una stima della "facilità" di trasmissione e man mano assegnerà SF più bassi, fino ad arrivare a quello minimo per ricevere correttamente.
   Non è possibile assegnare a tutti l'SF massimo perché a discapito della sicurezza di trasmissione/arrivo, sfrutta più potenza, quindi più consumi ed è più lento, al contrario un SF basso (SF6) sarà veloce ed efficiente, ma più soggetto a perdita di segnale e disturbi

3. Spiegare come funzionano, e quali sono le differenze, tra una multiplazione a divisione di tempo **TDMA** (Time Division Multiple Access), e una multiplazione a divisione di frequenza **FDMA** (Frequency Division Multiple Access). (14/01/22)

   TDMA e FDMA sono due tipologie di multiplazione diverse, ma che funzionano su uno stesso concetto: dividere un mezzo tra vari utenti.
   Nella TDMA il mezzo diviso è il tempo, viene permesso ad ogni stazione di trasmettere solo per un breve periodo (duty cycle), in tal modo tutti possono trasmettere equamente nel tempo utilizzando lo stesso mezzo fisico, nella FDMA invece ciò che si divide è la frequenza su cui si trasmette, sappiamo

bene che un segnale è trasportato da una portante (carrier) che è la freq base assegnata alle varie stazioni, questa portante in FDMA è diversa per ogni utente/stazione; il problema di assegnare una freq ad una stazione piuttosto che ad un'altra è che non tutte sono uguali, una F più bassa è in grado di arrivare più lontano, ma tramette più lentamente di una F alta che però viene bloccata facilmente da muri o altri impedimenti, per questo motivo si parla di Frequency hopping, un sistema che permette di avere F diverse in tempo diverso e quindi non penalizzare nessuna stazione, perché tutte prima o poi avranno utilizzato tutte le F disponibili sul canale

4. Descrivere il principio di funzionamento di un convertitore analogico digitale (ADC) per board Arduino. (03/02/22) (14/01/22)

   Un convertitore ADC si basa sul concetto di campionamento, prendiamo un segnale più o meno regolare e lo campioniamo, cioè prendiamo il suo valore in determinati istanti, più è alta la frequenza di campionamento, più sarà precisa la rappresentazione digitale del segnale analogico.
   L'aliasing è il fenomeno in cui la frequenza di campionamento è bassa e quindi abbiamo una rappresentazione non veritiera del segnale analogico, quindi si tende a prediligere una frequenza di campionamento alta, la quale però non è sempre un vantaggio in quanto necessita di potenza computazionale maggiore e il dato acquisito sarà più pesante, è quindi necessario avere un buon rapporto tra F massima del segnale e F di campionamento.
   Il modo per risolvere tale problema è utilizzare il teorema del campionamento di Nyquist, secondo il quale la F di campionamento deve essere maggiore del doppio della F massima del segnale, in altre parole dobbiamo acquisire più di 2 punti del segnale per ogni periodo.
   In particolare, l'arduino (o wemos) ha un convertitore a 10 bit, ciò significa che il segnale potrà essere acquisito (in ampiezza e quindi risoluzione) in 2^10 cioè 1024 intervalli.
   I classici 5V di lavoro dell'arduino, se inseriti come segnale analogico avranno una risoluzione massima di circa 5mV

5. Nella tecnologia WiFi IEEE 802.11, quali sono le principali differenze tra le due modalità di funzionamento, Infrastructure BSS e Independent BSS? (03/02/22)

   Nel wifi sono presenti due modalità di funzionamento: infrastrutturata e indipendente (normalmente chiamata ad-hoc)
   La prima si basa sull'idea di un singolo punto di collegamento (Accesso Point AP) che tiene attiva la rete e permette la connessione alle stazioni mobili (MS), in alcuni casi, per la versione extended possono essere aggiunti altri AP che però estendono la rete invece di crearne una nuova
   La seconda funziona con un collegamento diretto tra la stazioni

I vantaggi della modalità infrastrutturata rispetto alla indipendent sono che mantiene sempre la rete attiva, nel caso arrivino pacchetti destinati ad una stazione in sleep o comunque non attiva, vengono salvati per poi essere strasmessi, gestisce il risparmio energetico, ma si ha un doppio utilizzo della rete, in quanto quando la stazione A deve mandare un pacchetto alla stazione B, non la invierà direttamente anche se accanto, ma lo manderà all'AP che si occuperà di inoltrarlo al B, quindi con un delay maggiore, cosa che non accade nella modalità Ad-hoc, dove i pacchetti passano direttamente dalla sorgente al destinatario

6. Descrivere il sistema di cifratura dei pacchetti utilizzati nella rete LoRaWAN. (03/02/22)

   Nelle reti LoRaWAN vista la loro infrastruttura è necessario che tutti i pacchetti che transitano siano cifrati, ma allo stesso tempo passando nel network server, che deve smistare i pacchetti verso gli application server è necessario che il Net S sia in grado di verificare la reale provenienza dei pacchetti e leggere a chi sono destinati, ciò avviene secondo due metodi diversi.

   Firma: tutto il pacchetto viene inserito nel calcolo di un Hash basato sulla Network-Server Key NwkSKey, chiave detenuta dal device e dal Network server, il quale all'arrivo del pacchetto, verifica l'hash controllando quindi l'identità del device

   Cifratura: il solo payload viene cifrato con l'AppSKey, Application-Station Key, detenuta da device e application server, ciò fa sì, che il net server (che inoltra i pacchetti) e chiunque sia a lui collegato sia impossibilitato a leggere il contenuto del payload, ma al massimo potrà vedere da chi è partito e a chi è destinato

   Al collegamento del device alla rete seguono i passaggi per autenticarlo

   Il dev manda al network server una richiesta di connessione Join request contenente il proprio DevEUI, AppEUI e AppKey; il net server a quel punto risponde con una join accept contenente il DevAddress che userà il dispositivo, verrà anche chiesto al join server (terzo elemento estraneo al passaggio dati, ma "fidato") di generare le chiavi necessarie alla cifratura dei pacchetti, in tal modo non sarà il Network server a generarle e gestirle, ma potrà solo leggere ciò che è firmato con la NwSKey, quindi la AppSKey viene mandata al device e all'application server rendendo così la rete sicura

7. Spiegare le principali differenze tra un microcontrollore e un microprocessore. (03/02/22)

   microprocessore è un dispositivo utilizzato in sistemi come i PC che utilizza un bus dati esterno per connettersi agli altri dispositivi (ram, rom ecc), ha una capacità di calcolo elevata e può sostenere un sistema operativo

   Un microcontrollore (SoC) invece è un sistema che contiene un microprocessore, le ram e tutti gli altri elementi necessari al funzionamento, con bus interno. Al contrario del microprocessore, ha spesso

poca potenza di calcolo, ma consumi ridotti, il che lo porta ad essere preferibile quando le operazioni da svolgere non sono complesse

8. Descrivere il principio di funzionamento delle modulazioni digitali ed entrare nel dettaglio di una di loro (a scelta). (24/01/22)

   Le modulazioni digitali sono utilizzate per trasmettere segnali digitali, per farlo si usano svariati metodi, ma tutti accomunati dall'utilizzo di "simboli" cioè particolari forme/variazioni del segnale che indicano uno stato logico 0 o 1

   Le più usate sono Amplitude Shift Key ASK, Frequency Shift Key FSK, Phase Shift Key PSK

   In particolare la PSK, cioè la modulazione di fase, al contrario di quella analogica che spostava in uno spettro continuo la fase, in questo caso la ribalta totalmente

   Ci sono principalmente due modi per farlo, per indicare uno stato logico di sa una fase e l'opposta per l'altro, oppure utilizzare la variazione di fare per indicare uno stato logico, ad esempio per 00110 la fase rimarrà la stessa nel caso in cui da un bit 0 si passi ad un altro bit 0, ma varierà per il primo bit 1, al successivo varierà di nuovo e per lo 0 resterà il precedente

9. Riassumere il meccanismo di backoff esponenziale per le reti IEEE 802.11. (24/01/22)

   Nelle reti WiFi per evitare la collisione tra pacchetti trasmessi da stazioni diverse, si utilizza un sistema di Backoff, per evitare che il DIFS (un tempo che le stazioni devono aspettare per trasmettere) sia uguale per tutti creando una collisione, si utilizza un tempo di backoff, cioè un ulteriore tempo in cui le stazioni devono rimanere ferme in attesa prima di trasmettere, il problema subentra quando si perde un pacchetto e la finestra (il tempo) del backoff deve essere calcolato, avendo un calcolo esponenziale, cioè 2^m*(valore casuale) dove m è il numero di pacchetti persi, ad ogni perdita (e quindi ritrasmissione) la finestra aumenterà del doppio, creando quindi una situazione in cui una stazione dovrà aspettare un tempo indefinito

10. Descrivere le tre classi di funzionamento dei device LoRaWAN (24/01/22) (21/01/21)

    I device LoRa possono funzionare in 3 classi, queste non sono impostate in fabbrica, ma possono essere scelte durante l'utilizzo

    Classe A, il device è sempre in sleep (quindi non può ricevere) tranne mentre trasmette e per un certo tempo stabilito ad una certa distanza dalla trasmissione

    Clase B, include la Classe B ed aggiunge la possibilità di contattare il device a tempi stabiliti successivi ad un beacon (pacchetto sentinella utilizzato per sincronizzare)

    Classe C, utilizzando lo stesso principio dei Beacon della classe B, schedula dei momenti tra un beacon e l'altro in cui può ricevere un ping (pacchetto sentinella che precede una trasmissione) ad intervalli regolari, utilizza il beacon perché essendo tempi molto brevi è necessario che gli orari siano sempre perfettamente sincronizzati tra i vari device

11. Spiegare sinteticamente il funzionamento del protocollo MQTT (24/01/22) (21/01/21)

    L'Message Queuing Telemetry Transmission o MQTT è un protocollo utilizzato nell'IoT in alternativa al classico sistema client-server

    Di base esiste un server MQTT chiamato Broker che si occupa solo di smistare e collegare i messaggi, più come un Acces point che come un server che contiene le informazioni.

    Oltre al Broker ci sono i vari client che però possono essere connessi in due modi: Pubblish e Subscribe, in breve, chi deve trasmettere, quindi le schede connesse a sensori/attuatori, si connette in modalità Pubblish con un certo topic, cioè un argomento che identifica il tipo di messaggi che manderà, l'altra tipologia, il Subscribe invece serve a ricevere i messaggi del topi scelto, quindi verrà utilizzata per i device di monitoraggio, uno smartphone/pc ecc

12. Che cosa è un beacon in una rete 802.11? chi lo trasmette? (21/01/21)

    Le reti 802.11 per funzionare hanno bisogno di essere "viste" dai device che si vogliono connettere, per far ciò è necessario in qualche modo mettere in mostra l'esistenza della rete, si usano i beacon, cioè dei pacchetti segnalatori trasmessi in broadcast su tutta la rete a tempi regolari (schedulati, ma che in caso di trasmissione sovrapposta ad un'altra possono essere traslati) che vengono quindi ricevuti dai device sia già connessi, sia quelli che devono inserirsi nella rete e che tramite le conoscenze apprese (solitamente l'SSID) possono far richiesta per collegarsi

13. Spiegare quali sono e a cosa servono gli stati di funzionamento di un dispositivo che implementa la tecnologia Bluetooth. (21/01/21)

    Le

14. Spiegare sinteticamente la modulazione di tipo OFDM e in quali casi è impiegata

    La modulazione OFDM è basata sulla trasmissione di un segnale multi bit in contemporanea, ciò viene fatto modulando tramite la QAM (modulazione in cui si modificano l'ampiezza e la fase a 90° per inserire più bit in un solo simbolo) il segnale da trasmettere con segnali ortogonali tra loro, viene trasportato da portanti le cui frequenza saranno una il doppio dell'altra.

    Il segnale in QAM verrà codificato in n sottoportanti che tramite la trasformata inversa di Fourier (IFFT) verranno inserite in un segnale nel tempo (simbolo) e trasmesse, a quel punto potrà essere ricevuto il segnale e riconvertito tramite la trasformata di Fourier (FFT) in modulazione QAM e quindi sarà possibile tornare al segnale originale

    Alcuni degli utilizzi sono delle comunicazioni in fibra ottica, ADSL, ma anche nel WiFi

15.