Universitat de Girona
Escola Politècnica Superior

# Treball final de grau

**Estudi:** Grau en Enginyeria Informàtica

**Títol:** Anàlisi del trànsit Wi-Fi basat en Deep Learning per a la detecció d'un atac

**Document**: Resum

**Alumne**: Oliu Llorente Moragrega

**Tutor**: Lluís Fàbrega Soler
**Departament**: ATC
**Àrea**: ATC

**Convocatòria (mes/any):** Juny/2021

# Introducció i objectius

Les xarxes Wi-Fi són una popular tecnologia basada en el conjunt d'estàndards IEEE 802.11 que, pateixen de manera constant atacs a la seguretat de diversos tipus (p.e., d'obtenció de la clau de xifrat, de desassociació, de suplantació del Punt d'Accés, etc.), que atempten contra la privacitat i integritat de la informació i contra la disponibilitat de la xarxa.

Per identificar aquests atacs (i així potser evitar-los) s'utilitzen sistemes de detecció d'intrusions (Intrusion Detection Systems o IDS), que monitoren el trànsit de xarxa i l'analitzen fent servir diverses tècniques (comparació amb patrons d'atacs coneguts, comparació amb un model que representi una situació "normal", etc.) que permeten detectar si s'està produint un atac, de manera que es pugui actuar en conseqüència.

L'objectiu del projecte és dissenyar i implementar un programa que, basat en un dataset que contingui dades d'atacs Wi-Fi (AWID2) i una llibreria de Deep Learning (*fastai*), sigui capaç d'aprendre i detectar un tipus concret (ja definit) d'atac Wi-Fi.

# Metodologia i planificació

Per a realitzar el projecte s'hauran de realitzar una sèrie de passos tant d'aprenentatge i recerca com d'implementació. La majoria d'aquests passos són en ordre seqüencial, però alguns es podran fer en paral·lel (pe., els relacionats amb investigar, encara que sigui sobre temes diferents).

L'ordre dels passos és el següent:

1. Aprendre, investigar i assolir conceptes bàsics de Deep Learning i de la llibreria *fastai*.
2. Paral·lelament al pas 1, investigar i aprendre sobre els diferents atacs Wi-Fi (d'entre els atacs contemplats al dataset AWID2).
3. Decidir sobre quin atac fer el sistema de detecció en funció del que s'hagi après al pas 2.
4. Comprendre, interpretar i filtrar el dataset AWID2.
5. Construir el sistema de detecció d'atacs (del tipus escollit al pas 3).

6. Provar els resultats i la precisió del sistema.
7. Provar el sistema de detecció d'atacs en un escenari de laboratori.
8. Documentació i redacció de la memòria.

## Decisió de l'atac, la llibreria *fastai* i el dataset AWID2

Pel que fa a conceptes bàsics, destacar els 3 tipus de trames Wi-Fi:

- Les trames de gestió, que permeten als clients establir comunicació amb els AP i mantenir-ne la connexió (Figura 1). En són exemples les trames d'autenticació, associació, desautenticació, beacon, etc.

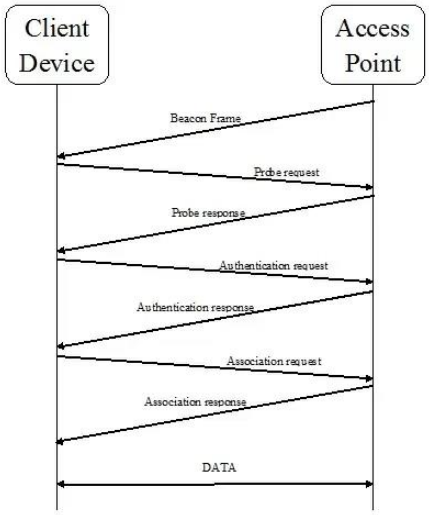


***Figura 1: Seqüència temporal d'una connexió a una xarxa Wi-Fi***

- Les trames de control, que coordinen l'accés al canal sense fils i participen en l'enviament de les trames de dades entre els AP i els clients.
- Les trames de dades, que transporten la informació com a tal (que prové d'altres capes). N'hi ha de diferents tipus en funció de si la informació s'envia en un servei basat en contencions, si porten informació addicional i/o si tenen temes de qualitat de servei (QoS).

Per a realitzar el projecte es necessitaran els següents recursos software:

- **Llibreria de Deep Learning *fastai***: És una llibreria gratuïta que permet dissenyar i implementar models de Deep Learning a "alt nivell".
- **Dataset AWID2**: És el dataset d'on s'extrauran les dades per a entrenar i testejar el model. És un dataset molt complet realitzat per a una universitat el qual consta de molta documentació i és utilitzat en molts projectes.

El dataset AWID2 (Aegean Wi-Fi Intrusion Dataset) conté el resultat de capturar el trànsit d'una oficina (simulada) on hi ha tant el trànsit resultat d'un ús normal de la xarxa com el trànsit resultant de realitzar una sèrie d'atacs sobre aquesta. Aquests atacs s'agrupen en atacs a la clau (com l'atac de força bruta), atacs al keystream (com l'atac ChopChop), atacs de denegació de servei (com l'atac de desautenticació) i atacs de "man in the middle" (com l'atac evil twin). D'entre aquests atacs es decideix basar el projecte sobre l'**atac de desautenticació**.

Aquest atac es basa en utilitzar (com el seu nom indica) les trames de gestió del tipus de desautenticació. Aquestes trames les envia l'AP cap a un client, que quan la rebi es desconnectarà automàticament de la xarxa (Figura 2).

L'atac aprofita el fet que les trames de desautenticació no estan protegides (no estan xifrades) i es poden suplantar. D'aquesta manera, l'atacant envia una trama falsa a la víctima fent-se passar per l'AP.

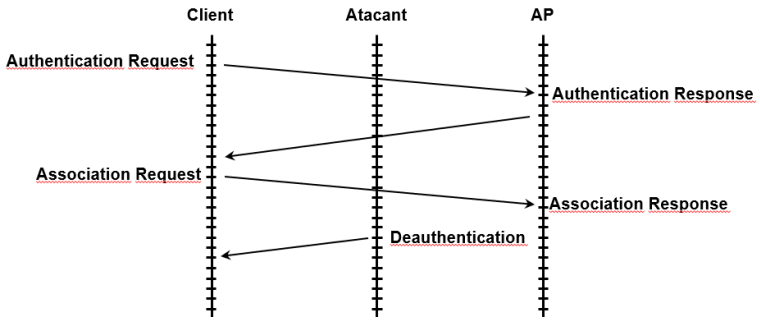


***Figura 2: Exemple del funcionament d'un atac de desautenticació***

# Anàlisi, disseny i implementació

El disseny del programa es basarà en 3 grans blocs (Figura 3). El bloc d'input, el bloc d'entrenament i el bloc d'output.

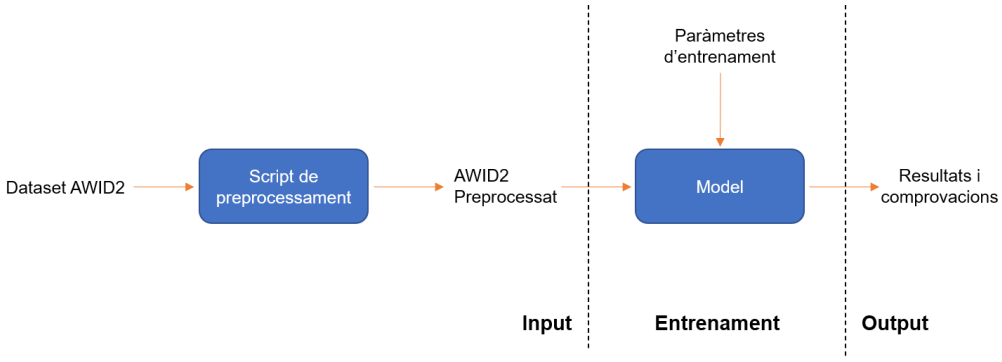


***Figura 3: Diagrama de blocs del programa***

El primer pas és preprocessar les dades de manera que el sistema de detecció les pugui llegir i utilitzar correctament. Per fer això es fa servir un script en Python que filtra el dataset AWID2 i deixa només les columnes i files que són realment necessàries per tal de detectar un atac de desautenticació.

A la part d'implementació es desenvolupa el programa de detecció mitjançant Python 3 i la llibreria *fastai*, on es crea un model de Deep Learning que aprèn de les dades preprocessades anteriorment (un 80% de les dades s'usen per entrenar el model i el 20% restant per a validar-lo). Es realitzen diverses proves al model per comprovar que s'ha creat correctament (pe., veure'n la learning rate, comprovar si hi ha overfitting...).

## Resultats i conclusions

Per validar el model, se n'extreuen una sèrie de mètriques que en permetin fer una anàlisi representatiu del funcionament.

Els resultats han sigut:

- 3056 paquets classificats com a part d'un atac, amb més d'un 70% de precisió, i 1.790.546 paquets classificats com a paquets que no formen part de l'atac, amb un 99.5% de precisió.
- 2158 paquets maliciosos classificats correctament de 10447 que n'hi ha en total, i 1.782.257 paquets no maliciosos classificats correctament d'1.783.155 que n'hi ha en total.
- 898 falsos positius i 8289 falsos negatius.

Com a conclusió, es pot veure que els resultats en general són bons. Els percentatges d'encert estan molt bé (sobretot per la part de paquets no maliciosos) i no surten gaires falsos negatius. Però si que és cert que surten més falsos positius del que s'esperaria (cosa a millorar en el treball futur).

Com a treball futur quedaria analitzar més a fons el dataset i aprofundir més en la creació del model per tal de millorar-ne els resultats (com els falsos negatius).

També acabar la part de provar el sistema amb dades provinents d'un atac simulat en un entorn nostre, ja que tot i que s'ha pogut reproduir l'atac, no s'han pogut passar les captures a un format apte per al model.