Redes de Ordenadores para Robots y Máquinas Inteligentes
Práctica 5: WIFI

Departamento de Teoría de la Señal y Comunicaciones y Sistemas Telemáticos y Computación
URJC

Abril de 2024

Para realizar esta práctica se necesita el emulador de redes **Mininet-Wifi**. Tienes 2 opciones:

1. Puedes usar la máquina virtual mininet-wifi-ror.ova, que es una máquina Ubuntu con Mininet-Wifi ya instalado, preparada para importar directamente en VirtualBox.

   Puedes descargarla de: `https://mobiquo.gsyc.urjc.es/mininet-wifi-ROR.ova`

   Para entrar en el Ubuntu de la máquina virtual, el usuario es 'ror' y la contraseña 'ROR20ROR'.

2. Puedes instalar Mininet-Wifi en nativo en tu ordenador con Ubuntu con los siguientes comandos:

```
sudo apt install git
sudo apt install python-is-python3
git clone https://github.com/intrig-unicamp/mininet-wifi
cd mininet-wifi
sudo util/install.sh -Wlnfv
```

Descarga tus escenarios de red para la práctica del siguiente enlace:
`https://mobiquo.gsyc.urjc.es/practicas/ror/p5.html`
y descomprime el fichero `lab-wifi.tgz`.

1. Escenario simple

En el fichero `escenario_simple.py` se encuentra definida una topología de red para Mininet Wifi. Muévete a la carpeta donde has descomprimido el escenario `lab-wifi` y verás tres ficheros y una captura. El escenario se arranca de la siguiente forma:

```
sudo ./escenario_simple.py
```

El diagrama muestra las posiciones de cada uno de las estaciones y los APs. Fíjate en el alcance que tienen ap1 y ap2 y piensa a qué APs estarán conectadas cada una de las 3 estaciones.

1. Para saber qué interfaces de red tienen los APs y las estaciones, ejecuta el comando `net` desde la interfaz CLI y anota qué interfaces de red ha creado mininet-wifi para cada uno de los dispositivos [1].

[1] Aunque no aparecen las interfaces de loopback para las estaciones, éstas sí existen

2. Desde la interfaz CLI de mininet-wifi arranca un terminal para `sta1` y desde ese terminal ejecuta el comando que muestra la configuración IP de esa estación y apunta la dirección MAC y dirección IP.

3. Ejecuta el comando que muestra la información de la interfaz inalámbrica en `sta1`. Fíjate en la información sobre el modo de conexión, el SSID al que está conectado y el canal.

4. Obtén la misma información de `sta2`, `sta3` y realiza una tabla que resuma los datos de las 3 estaciones:

Dispositivo	Interfaz inalámbrica	Dir. MAC	Dir. IP	Tipo de conexión	SSID	Canal

5. Como `sta1` y `sta2` están asociadas al mismo AP hay conectividad entre ambas estaciones, pero no hay conectividad con `sta3` porque no se ha configurado una red que conecte ambos AP. Para comprobarlo lanza wireshark en `sta1` (lo puedes lanzar en background o crear otro terminal para `sta1`) y selecciona la interfaz inalámbrica de `sta1`. A continuación ejecuta un `ping` para que envíe 3 paquetes a `sta2` y después otro `ping` para que envíe 3 paquetes a `sta3`. Interrumpe la captura y guarda su contenido en el fichero `wifi-01.cap`. Explica en la memoria el contenido de la captura.

En los mensajes capturados verás que las cabeceras que aparecen en el nivel de enlace tienen el formato de mensajes Ethernet, y no se muestran las cabceras del protocolo 802.11. Normalmente los drivers de las tarjetas inalámbricas transforman el paquete 802.11 en formato 802.3 (Ethernet). Para poder analizar el tráfico 802.11 es necesario hacer uso de una interfaz especial que crea mininet-wifi para procesar el tráfico inalámbrico.

Desde la máquina real ejecuta:

```
sudo ifconfig hwsim0 up
```

Lanza Wireshark seleccionado esta interfaz para realizar la captura. En esta interfaz se pueden capturar todos los mensajes de `ap1` y `ap2`. Vamos a provocar una nueva asociación de `sta1` a `ap1` para ver todos los mensajes 802.11.

Desconecta `sta1` de la red `ssid1` que es en la que se encuentra asociada y verifica que ya no está asociada a dicha red.

Ahora reconectaremos la estación a `ap1` y capturaremos los mensajes intercambiado en el proceso de la asociación.

Después de pocos segundos verás como la estación y el AP han intercambiado mensajes. Interrumpe la captura y guarda el contenido en un fichero `wifi-02.cap`.

En la captura verás como los mensajes además de la cabecera 802.11 tienen más información que no forma parte de la trama 802.11. Son metadatos que llevan información del nivel físico y que pueden ser datos importantes para analizar la capturas: `Radiotap header` y `802.11 Radio information`.

Analiza la captura:

6. Selecciona un mensaje de baliza enviado por el `ap1`, dirección Ethernet de origen `00:00:00:00:00:01`:

   a) Indica qué canal está utilizando para transmitir, la tasa de envío y la frecuencia utilizada.

   b) Indica los valores de los bits `To Ds` y `From DS` que viajan en el campo `Flags` del campo `Control Field`:

   c) Teniendo en cuenta los valores anteriores, indica los valores de las 3 direcciones MAC que lleva la trama baliza y explica a qué máquinas corresponden. Comprueba en la interfaz hexadecimal de wireshark que las 3 direcciones van una a continuación de la otra, después está el número de secuencia (2 bytes) y que detrás no hay un campo para la 4ª dirección.

d) ¿Por qué crees que el número de secuencia de una trama baliza es siempre 0?

e) Indica cuál es el intervalo entre tramas baliza

f) Indica cuál es el SSID que se está usando.

g) Busca en el campo `Capabilities` algún campo que indique que el dispositivo que está transmitiendo es un AP.

7. Selecciona el primer mensaje `Probe Request` de `sta1`:

   a) Explica los valores del campo `To DS` y `From DS` y las 3 direcciones y a qué máquinas se refiere.

   b) Fíjate si el mensaje `Probe Request` lleva en alguna cabecera el SSID al que se quiere conectar y el canal.

   c) ¿Por qué crees que hay varios mensajes `Probe Request`?

8. Selecciona el mensaje `Probe Response`:

   a) Explica qué valores tienen los posibles 4 campos de direcciones y a qué máquinas se refiere.

   b) Indica qué campo muestra el canal en el que el AP está realizando la respuesta.

   c) Indica qué campo muestra el SSID que está usando el AP.

9. Fíjate que después del mensaje `Probe Response` hay un asentimiento dirigido a `ap1` para confirmar la recepción de `Probe Response`. Observa que los asentimientos en wifi no indican el número de secuencia que se asiente, por lo que asienten la última trama recibida, y el emisor no enviará otra trama hasta tener asentida la anterior. ¿Cuántas direcciones lleva el mensaje de asentimiento?

10. Selecciona el mensaje `Authentication` que envía la estación:

    a) En la asociación no están usando autenticación, indica donde se muestra esta información y el número de secuencia asociado a la fase de autenticación, fíjate que es diferente del número de secuencia de la cabecera general de 802.11 (`Sequence Number`).

11. Selecciona el mensaje `Authentication` que envía el AP:

    a) Comprueba que lleva el mismo algoritmo de autenticación que la solicitud y comprueba el número de secuencia asociado a la fase de autenticación.

    b) Observa que ambos mensajes de autenticación están asentidos, fíjate que sólo se distinguen por la dirección destino.

12. Comprueba en el mensaje `Association Request` que viaja el SSID y el Listen Interval. Recuerda que el Listen Interval está expresado en número de intervalos de envío de tramas baliza. Además comprueba que el número de secuencia de la cabecera general de 802.11 es uno más que el del mensaje de autenticación enviado por `sta1`.

13. Identifica el AID (Association ID) que viaja en el mensaje `Association Response`. Y comprueba que el número de secuencia de la cabecera general de 802.11 es uno más que el del mensaje anterior enviado desde `ap1`.

14. Desde el terminal de la estación `sta1` realiza un escaneo para ver que redes inalámbricas son visibles desde ese punto y realiza lo mismo desde `sta2` y `sta3` (el escaneo tarda unos segundos). Anota la potencia de señal recibida de cada AP.

15. Para saber la distancia desde cada AP a las estaciones ejecuta el siguiente comando en la interfaz CLI mininet-wifi, por ejemplo para ver la distancia entre `sta1` y `ap1`:

    ```
    mininet-wifi> distance sta1 ap1
    ```

    Compara estas distancias de cada estación con los AP con los que tiene visibilidad y con la potencia de señal recibida en cada estación.

16. Con el siguiente comando vamos a mover a `sta1` a otra coordenada fuera del alcance de cualquier AP y sta. Elige tú la coordenada (X,Y) y ejecuta lo siguiente en la interfaz CLI de mininet-wifi:

    ```
    py sta1.setPosition('X,Y,0')
    ```

    Comprueba la nueva posición en el dibujo. Y ejecuta un escaneado para ver que ya no tiene alcance a ningún AP y estación.

17. Mueve la estación `sta1` a esta nueva posición (120,20,0), fíjate en la figura que muestra mininet-wifi y comprueba desde el terminal de `sta1` que se ha asociado con `ap2`. También comprueba que ahora puede comunicarse con `sta3` pero no con `sta2` ya que ahora `sta1` estará asociada a `ap2` (al igual que `sta3`). Y aunque `sta2` podría estar asociada a `ap2` porque se encuentra en su radio de acción, `sta2` está asociada a `ap1` por recibir su señal con una potencia algo mayor.

18. Lanza una nueva captura en la interfaz `hwsim0` y realiza desde `sta1` un `ping -c 3` a `sta3`. Una vez terminada la ejecución del `ping` interrumpe la captura y guárdala en el fichero `wifi-03.cap`. Analiza el contenido y explica los mensajes que son consecuencia de la ejecución del `ping`:

    a) ¿Cuántos mensajes ICMP echo request hay? ¿Y cuántos ICMP echo reply? ¿Por qué?

    b) Fíjate en las direcciones que llevan estos mensajes y justifica sus valores.

    c) Observa los mensajes de asentimiento. Explica qué mensaje asiente cada asentimiento.

2. Tramas RTS/CTS

Dentro del entorno de simulación mininet-wifi no se envían nunca utilizando tramas RTS/CTS (Request to Send, Clear to Send). Para ver estas tramas carga el fichero de captura `rts-cts.cap` en Wireshark.

1. Observa los mensajes 1 y 2 e indica la dirección MAC de la estación que tiene datos que enviar y la dirección MAC de la estación que está concediendo el permiso.

2. ¿Cuál es el mensaje que lleva los datos?

3. En el mensaje 3 observa la cabecera IEEE 802.11, en la pestaña `Flags`, indica si se puede saber que el nodo que está transmitiendo es un AP o una estación, y si los datos están protegidos (cifrados). Observa que si los datos fueran en claro, se podrían examinar las siguientes cabeceras de la pila TCP/IP, cosa que aquí no sucede.

4. El mensaje 4 es un asentimiento de un conjunto de datos `Block ACK`. Dentro de la pestaña `Compressed BlockAck Response` va codificado el conjunto de tramas que asiente.
   El `Block Ack Bitmap` es un campo donde cada bit representa si se ha recibido ACK (1) o no se ha recibido (0) una trama concreta. Con los 8 bytes de este campo (64 bits) se pueden identificar 64 tramas, es decir, se puede indicar si se ha recibido o no 64 números de secuencia comenzando en el número de secuencia especificado en `Starting Sequence Number`. A la vista de este campo, indica qué número/s de secuencia se están asintiendo.

5. Analiza el campo `Duration` de los mensajes 1, 2, 3 y 4.

6. Los mensajes 5 y 7 no llevan datos, indican respectivamente que el dispositivo se va a suspender (modo de baja energía) y se va a despertar. Despliega la pestaña `Flags` e indica la diferencia que ves entre ellos.

3. Autenticación

Arranca el escenario:

```
sudo ./authentication.py
```

1. Desde la interfaz `mininet-wifi>` puedes ver la configuración de red que se ha arrancado, para ello ejecutamos el comando `dump`. Anota las interfaces y direcciones IP de cada dispositivo. Deberías identificar 2 estaciones y un AP.

2. Consulta a qué SSID están asociados `sta1` y `sta2`.

3. Activa la interfaz `hwsim0` y lanza una captura. Los nodos `sta1` y `sta2` ya han realizado la fase de asociación con el AP. Para ver el proceso de intercambio inicial de los mensajes entre una estación y el AP vamos a desconectar y conectar la interfaz inalámbrica de `sta1`:

   ```
   ifconfig sta1-wlan0 down
   ifconfig sta1-wlan0 up
   ```

   A los pocos segundos observarás que se han intercambiado mensajes para la autenticación y asociación de `sta1`. Interrumpe la captura y guarda el contenido en el fichero `wifi-04.cap`.

   Selecciona el mensaje `Authentication` que envía la estación. ¿Qué algoritmo de autenticación se está usando?

4. Identifica los 4 mensajes para el intercambio de información de claves. Explica qué tipo de trama 802.11 tienen estos mensajes y su estructura de cabeceras. En particular, indica para qué sirve el campo `Type` de la cabecera LLC y que valor lleva.

5. Para cada uno de esos 4 mensajes, identifica los campos importantes que deberían llevar y anota sus valores: ANonce, SNonce y direcciones MAC de los dos nodos. Recuerda que a partir de esta información y el secreto compartido a priori ("clave de la wifi") se derivarán las claves que se usarán en la sesión para cifrar los mensajes.

6. Verás a continuación algún mensaje dirigido a alguna dirección especial de IPv6 pero si seleccionas el mensaje no puedes ver su contenido. Es necesario descifrarlo. Selecciona en el menú de Wireshark "Visualización" → "Barra de herramientas de Wireless". En la nueva barra que ha aparecido en la interfaz, selecciona "Preferencias de 802.11" → "Decryption keys" → "Edit" e introduce un algoritmo con "Key Type" `wpa-pwd` y clave `123456789a`. Guarda los cambios y observarás que los mensajes de IPv6 se han descifrado pudiendo acceder a todas sus cabeceras. Explica qué tipo de trama 802.11 es este paquete IPv6, y qué tipo de paquete IPv6.

   Recuerda: para poder descifrar el tráfico 802.11 más allá de la cabecera 802.11 es necesario tener en la captura los mensajes de intercambio de claves (4-way-handshake) y conocer la clave de la wifi. A partir de esta información se pueden calcular las claves de sesión y descifrar el tráfico.

4. Red ad-hoc

En el modo ad-hoc no hay AP, y las estaciones se conectan entre ellas a un SSID y canal común. Arranca el escenario para analizar este modo de funcionamiento:

```
sudo ./simple_adhoc.py
```

1. Extrae la información de las direcciones IP de cada una de las estaciones y el SSID y canal que están usando.

2. Activa la interfaz `hwsim0` y realiza una captura. Indica qué estación o estaciones están enviando tramas `beacon`.

3. Mientras está capturando wireshark, ejecuta una prueba de ping entre todas las estaciones. Interrumpe la captura y guarda su contenido en el fichero `wifi-05.cap`. Explica los resultados obtenidos.

4. A la vista de la captura, piensa en qué diferencias hay con respecto al número de mensajes de ping que se ven, comparando la comunicación de dos estaciones con vibilidad directa en el escenario Adhoc y en un escenario en modo infraestructura.

5. `sta1` y `sta3` no se pueden comunicar directamente porque no tienen visibilidad, pero podrían hacerlo si `sta2` se comportara como un router. Para ello vamos a activar el encaminamiento en `sta2` y vamos a configurar un ruta en `sta1` y `sta3`:

   ```
   mininet-wifi> sta2 echo 1 > /proc/sys/net/ipv4/ip_forward
   mininet-wifi> sta1 ip route add 10.X.0.3 via 10.X.0.2
   mininet-wifi> sta3 ip route add 10.X.0.1 via 10.X.0.2
   ```

   Vuelve a iniciar la captura de tráfico, asegúrate de que las cachés de ARP de todas las máquinas están vacías [2] y realiza un ping desde `sta1` a `sta3` para que se envíen 3 Mensajes ICMP Request. Guarda el contenido en el fichero `wifi-06.cap`.

   Fíjate como `sta1` y `sta3` se comunican a través de `sta2` para ello puedes observar en los mensajes los campos de las direcciones en las tramas 802.11 y las direcciones utilizadas en los mensajes de ARP.

   Observarás mensajes `ICMP Redirect` que envía `sta2`: estos mensajes los genera la pila TCP/IP ya que en `sta2` se recibe un mensaje por la misma interfaz por la que debe reenviarlo, y en esta situación `sta2` avisa al origen por si éste puede comunicarse directamente con el destino. En un entorno inalámbrico estos mensajes no son de utilidad pues las estaciones `sta1` y `sta3` no tienen visibilidad directa. Sin embargo, esos mensajes van a provocar que desde `sta1` se envíe una solicitud de ARP directamente preguntando por `sta3`, a la que no puede haber respuesta porque no hay visibilidad directa.

   Explica el tráfico que observas como resultado del envío de un ICMP echo request desde `sta1` a `sta3` y su respuesta.

[2] Con el comando 'arp -a' puedes ver la caché de ARP. Con el comando 'arp -d direccionIP' borras esa dirección.

5. Normas de entrega

Es necesario entregar a través del aula virtual los siguientes ficheros:

- Memoria en formato pdf donde se explique razonadamente cada uno de los apartados de este enunciado.
- Fichero `p5.tgz` resultado de comprimir **una carpeta de nombre p5** que contenga en su interior los ficheros de captura de tráfico: `wifi-01.cap` hasta `wifi-06.cap`.