

# **Ataques de Denegación de Servicio en redes inalámbricas (Wi-Fi)**

---

# Ataques DoS en Wi-Fi

---

- **Las redes wifi son muchiiiiisimo mas vulnerables a DoS que las redes cableadas:**
  - **todos los ataques de redes cableadas**
  - **mas todos los específicos de wifi:**
    - **Radio: jamming.**
    - **Autenticación: desasociaciones.**

# Ruido en conexiones inalámbricas

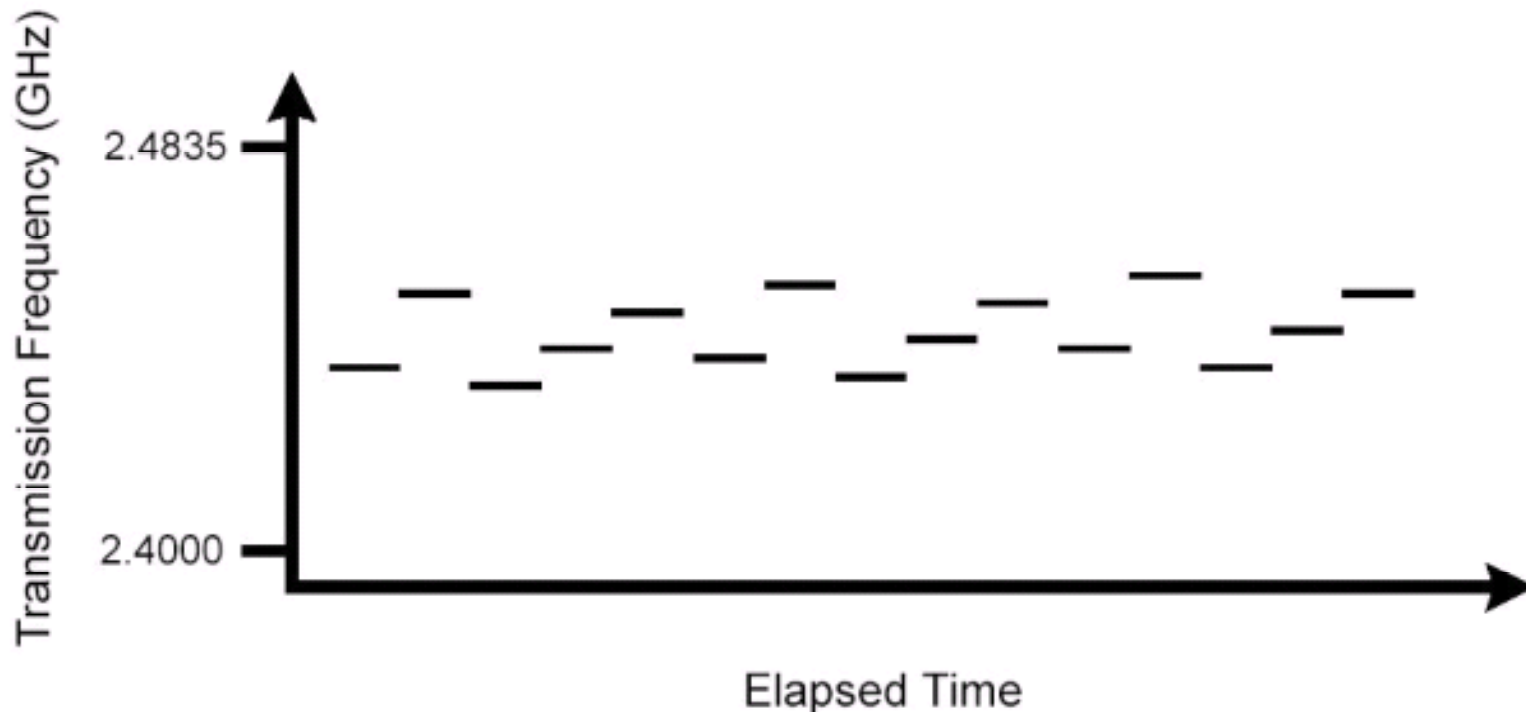
---

- Las redes inalámbricas no están pensadas para hacer corrección de errores, sólo para detectarlos.
- El mayor problema -> ruidos no provocados -> pérdida en la calidad de la comunicación, no su caída (voz).
- Ataque obvio: emitir ruido a una potencia brutal.
- **IMPORTANTE:** Un atacante tiene que gastar 1 / 10000 veces la potencia de un emisor normal. Basta con corromper un bit por paquete para que el checksum falle y haya que retransmitirlo.

# Ruido en conexiones inalámbricas

---

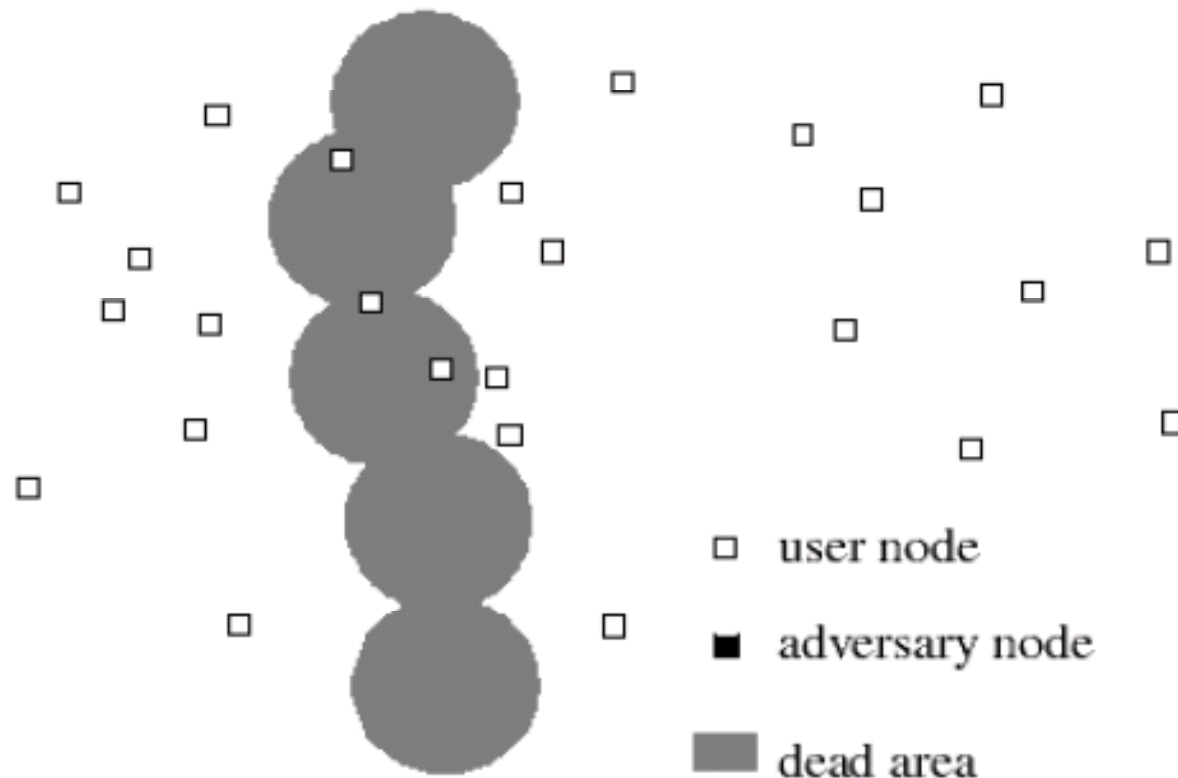
- El mecanismo más utilizado para evitar ruidos no deseados (anulación de la señal, en definitiva) es usar FHSS (Frequency Hop Spread Spectrum):



# Ruido en conexiones inalámbricas

---

- **Mejora: ahora la relación no es de 1 / 10000, sino que el atacante sólo afecta a los paquetes que sean emitidos en el rango atacado:**



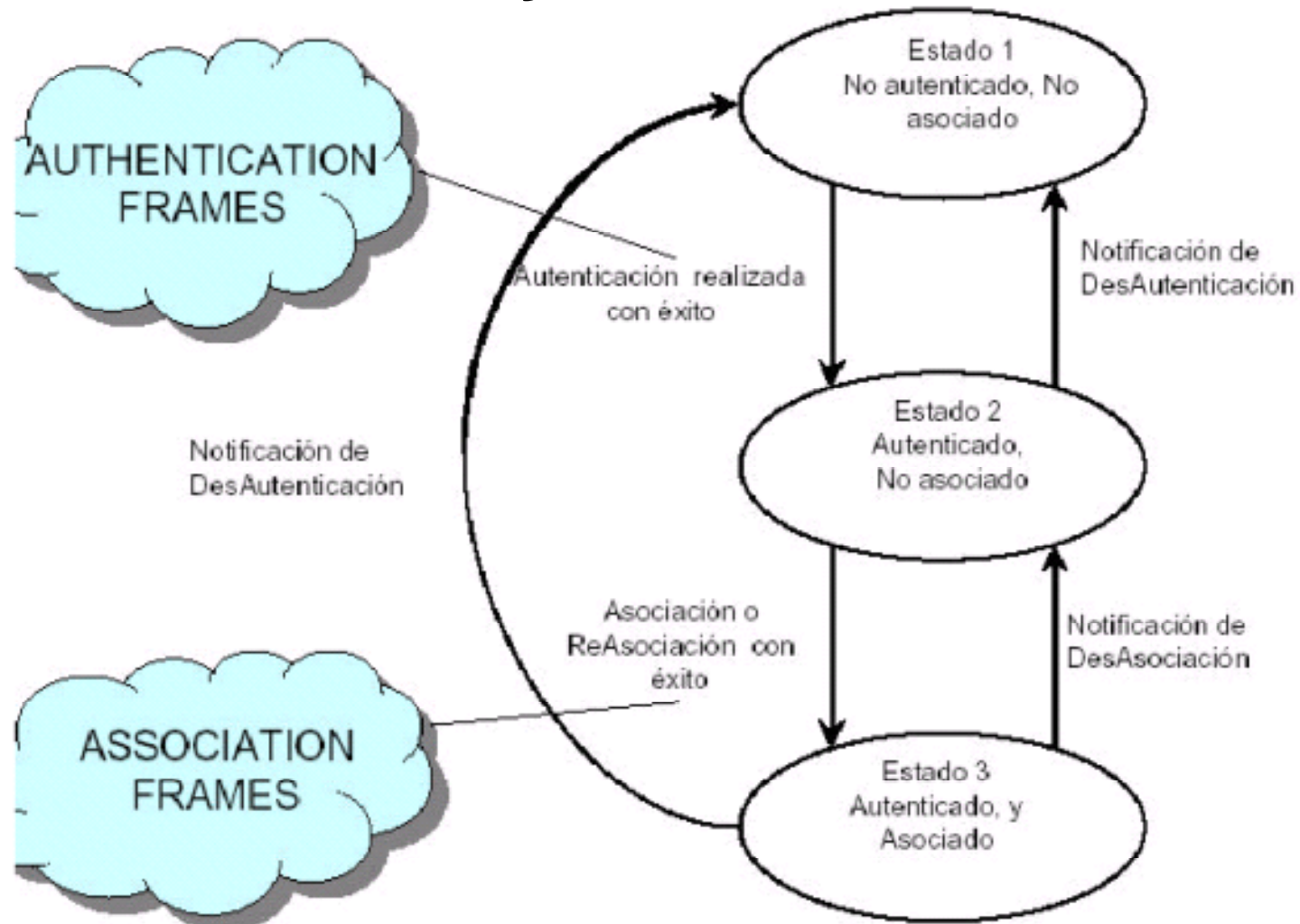
# El atacante contraataca!

---

- FHSS "cansa" al atacante -> centrarse en una conexión en concreto: sólo emite cuando haya datos que quiere denegar -> volvemos a una buena relación entre potencia necesaria para atacar / potencia necesaria para emitir.
- Solución implementar checksums para corregir errores, no solo para detectarlos.

# DoS por el funcionamiento Wi-Fi

- Proceso de asociación y autenticación a una red Wi-Fi:



# DoS por el funcionamiento Wi-Fi

---

- **Mecanismo manual:**
  - **Configurar nuestra tarjeta en modo Master y con la MAC del AP (con un sniffer)**
  - **Enviar tramas de desasociación:**

```
while true
do
    iwpriv wlan0 kickmac MAC
done
```

- **Ataque DoS masivo: MAC = FF:FF:FF:FF:FF:FF**

# DoS por el funcionamiento Wi-Fi

---

- **Herramientas automáticas:**
  - **airjack.c**
  - **fata-jack.c**

**(<http://www.blyx.com> para  
instalarlo en castellano ;-P)**

# ¿Preguntas?

---

```
if (bueno && breve)
    printf ("%d", bueno * 2);
```

```
O;-)
```