

ESP32 ORIENTADO AL VULNERABILIDAD DE REDES



ESRIC FREQUENCY TIM

Funcionamiento del Dispositivo

3

Se utiliza un microcontrolador ESP32 para ejecutar código que controla los módulos nRF24L01+.

Estos módulos son capaces de transmitir y recibir señales de radio en la banda de 2.4 GHz, la misma banda que utilizan muchos dispositivos inalámbricos.

Al enviar señales de radio aleatorias o paquetes innecesarios, el ESP32 interfiere con la comunicación de estos dispositivos.

```
JLANE rading intermercie
 1s Jarmming_liscte: ()
 Letser/nnleriegfles ();
 Stop, senfect: ();
 Retfact: +d)
 serffact: (tal);
 yoat of iefresyclemiett.atefactt)
 Pladia rerfect (scle_istrermating: 4 ref)
Whize: fhret_irestanct. (lacta: (t tadie flam
 Ntatle, leng_istefacic;
 C spicas-rircternitter: lef;
 Descrert idola hissiac:
 Inay hotiget! Jugnfitle tatal)
   Qg;
ister_lace seringlor
    Wieer: (b?
Reberis_jammiforentfer/les(etrentting incherranterm
JF Pesstnak corigrise, defercforris)
To be accepasementaration attacks, —Trogract for
Auct Radic: /estiernacfolhefergictzacing poramict
          cle≃trér(lescferming VOTT)
             er/agtifiet(swrettile
```

Técnicas de Interferencias

Jamming

Emite señales de radio fuertes que saturan el espectro, dificultando la comunicación entre dispositivos.

Spoofing

El dispositivo puede enviar paquetes de datos falsos, engañando a los dispositivos para que interpreten información incorrecta.

DoS

Ataques de denegación de servicio (DoS) pueden abrumar a los dispositivos con paquetes innecesarios, interrumpiendo su funcionamiento normal.



Conexiones Afectadas por el ESP32-BlueJammer



Audio

Puede interrumpir la reproducción de audio, causando distorsión o cortes en la señal.



Bluetooth y BLE

El dispositivo puede interferir con las conexiones Bluetooth y Bluetooth de baja energía (BLE), dificultando la comunicación entre dispositivos.



Redes Wi-Fi

Las conexiones Wi-Fi pueden
verse afectadas, causando
lentitud, interrupciones o pérdida
de conexión.



Impacto en Dispositivos IoT y

Otros Dispositivo	Frecuencia	Interferencia
Controles Nintendo Switch	2.4 GHz (Bluetooth)	Interrupción de conexión
Dispositivos IoT (Bluetooth)	2.4 GHz (Bluetooth)	Pérdida de conectividad
Dispositivos IoT (BLE)	2.4 GHz (BLE)	Interferencia en comunicación
Redes Wi-Fi	2.4 GHz (WiFi)	Pérdida de señal, lentitud
Drones RC	2.4 GHz	Pérdida de control



Aplicaciones y Uso del Dispositivo

Investigación

Estudiar la seguridad de las comunicaciones

inalámbricas.

Prueba de

Rennatar au ricondidades en sistemas

inalámbricos.

Educación

Demostrar los efectos de la interferencia

radioeléctrica.

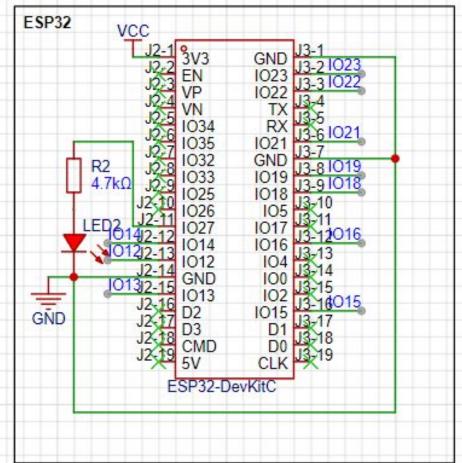
Uso Ilícito

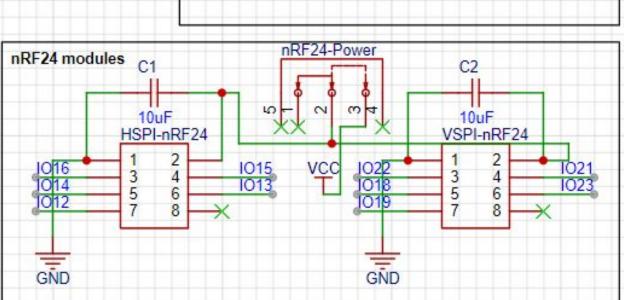
Interferir con comunicaciones sin autorización.

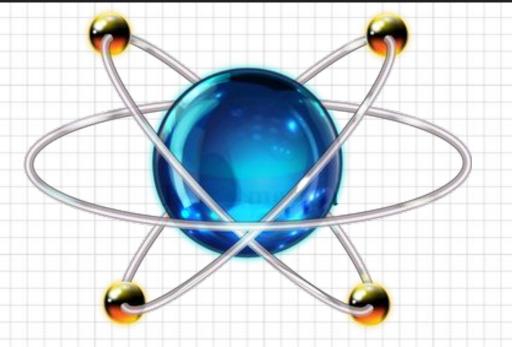
4

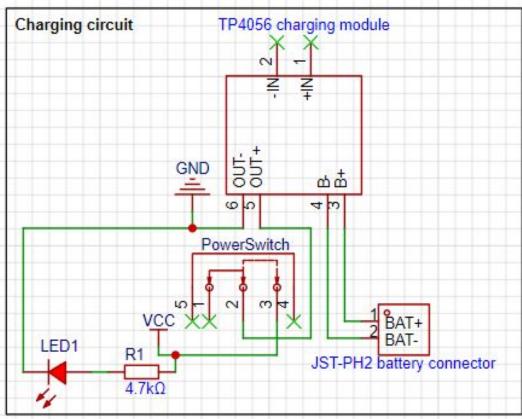
3













```
. .
```

wifi.cpp

```
void begin() {
        setPath("/web");
        setSSID(settings::getAccessPointSettings().ssid);
        setPassword(settings::getAccessPointSettings().password);
        setChannel(settings::getWifiSettings().channel);
        setHidden(settings::getAccessPointSettings().hidden);
        setCaptivePortal(settings::getWebSettings().captive_portal);
        if (settings::getWebSettings().use_spiffs) {
            copyWebFiles(false);
       mode = wifi_mode_t::off;
       WiFi.mode(WIFI_OFF);
        wifi_set_opmode(STATION_MODE);
        wifi_set_macaddr(STATION_IF, (uint8_t*)settings::getWifiSettings().mac_st);
        wifi_set_macaddr(SOFTAP_IF, (uint8_t*)settings::getWifiSettings().mac_ap);
```

