ANALISES E APLICABILIDADES DE UM JAMMER 2.4GHZ

Noilson Caio T. de Araújo
GTER 38 / GTS 24

SOBRE

Noilson Caio Teixeira de Araújo

Caiogore (at) gmail (dot) com

https://ncaio.wordpress.com

https://www.jammer4.com

MOTIVAÇÃO

- Curiosidade;
  - Como e por qual motivo usar ?
- Aprendizado;
  - Matar dúvidas !
- Compartilhar conhecimento;
  - Site.
- A natureza da banda ISM.

WWW.JAMMER4.COM

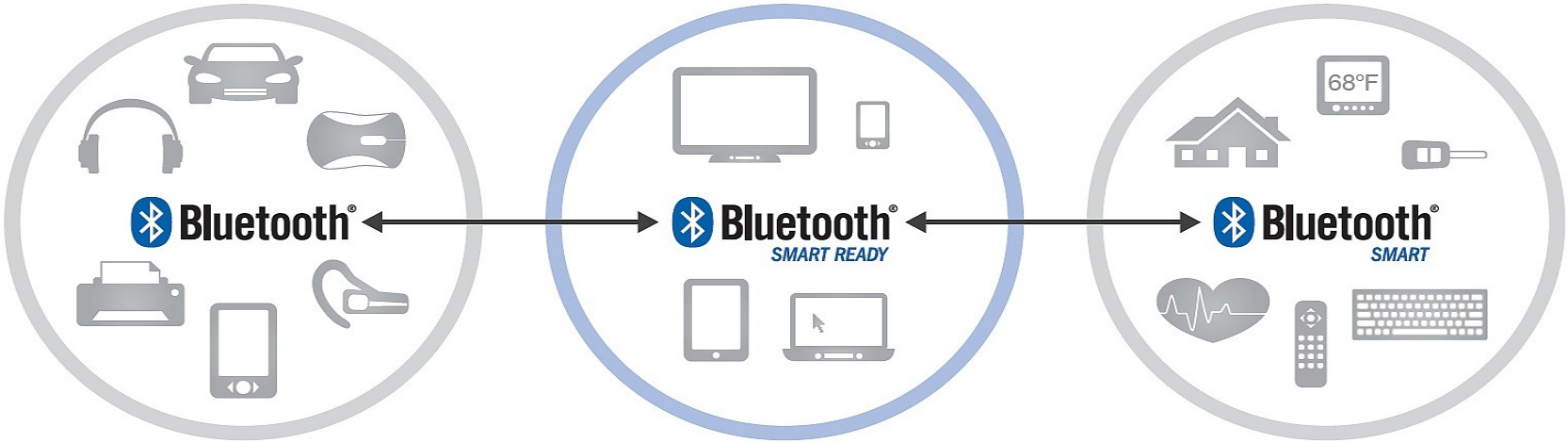
ESTE TRABALHO

Este documento é uma pesquisa independente e com fins exclusivamente educacionais. Não faz apologia a vandalismo ou atos de desordem, não tem fins comerciais, apenas educativos.

Este trabalho aborda análises, situações e cenários que envolvem o padrão 802.11b e 802.11g, exclusivamente na frequência 2.4Ghz.

+ Bluetooth

RFID E IDC (BLUETOOTH SMART)



BANDA ISM

Reserva de frequências não ‘protegidas’, conhecida como Industrial, Scientific, and Medical radio bands (ISM).

Existem pequenas parcelas de espectros reservadas a operações de radares.

… Vai da frequência central de 6.780 MHz a 245.000 MHz.

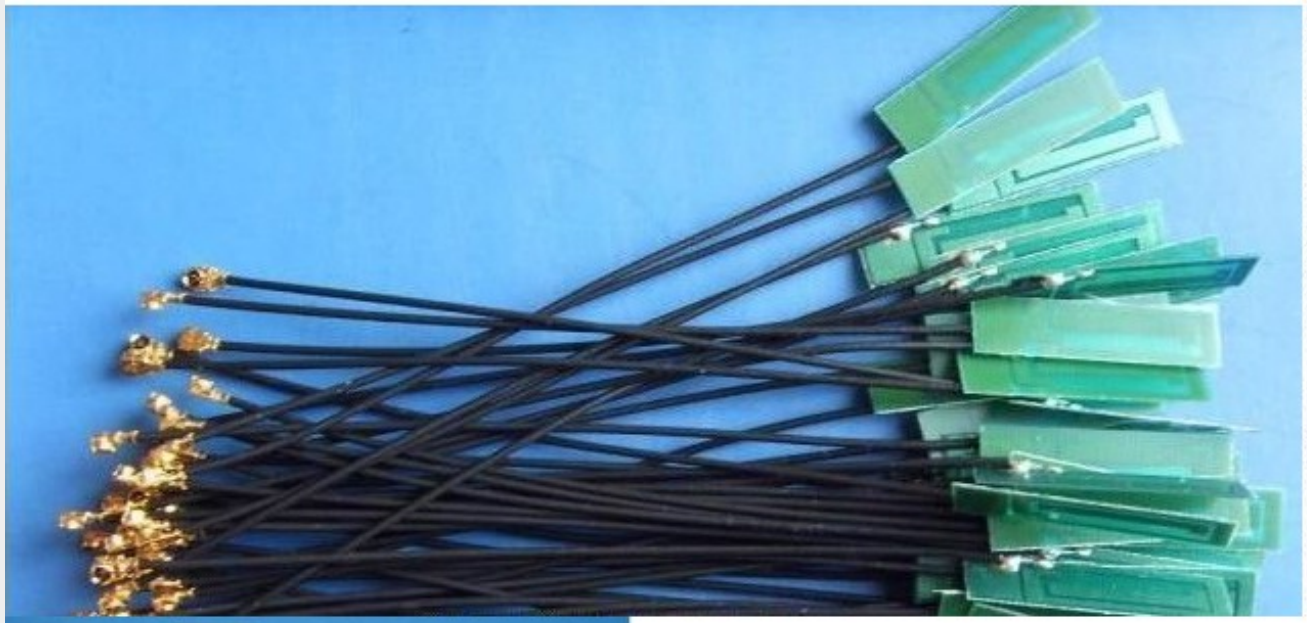
QUASE TUDO É ISM.

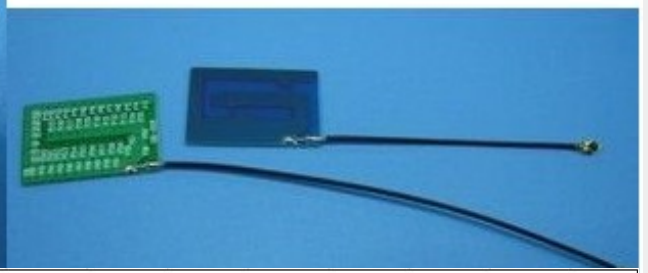
“You don't need a license to operate on them.”

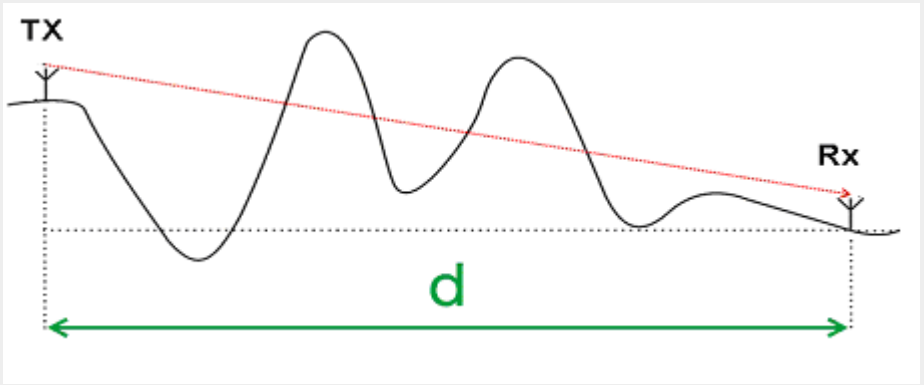
Giz Explains: Why Everything Wireless is 2.4GHz

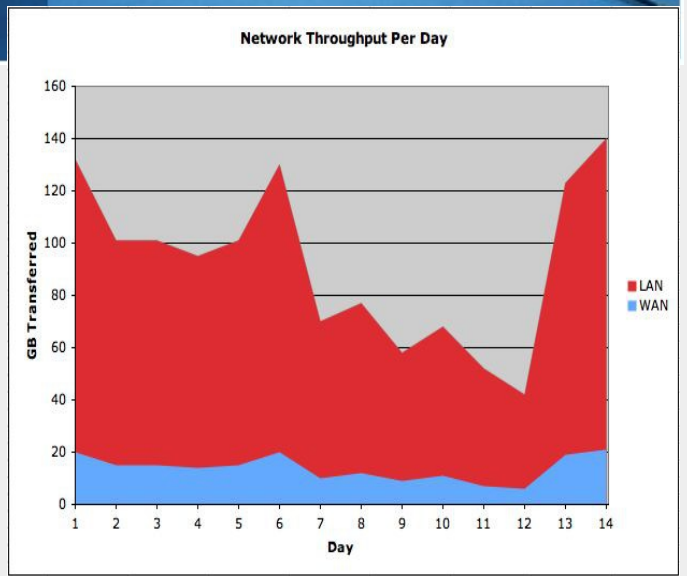
http://gizmodo.com/5629814/giz-explains-why-everything-wireless-is-24ghz

Por que 2.4 GHz?






TX
Rx
d


Network Throughput Per Day
GB Transferred
Day
LAN
WAN
0
20
40
60
80
100
120
140
160
1
2
3
4
5
6
7
8
9
10
11
12
13
14

Forno de microondas.

- 2.45GHz
- Dielectric

802.11a/b/g

Primeira regra: 2400MHz to 2483.5MHz

Para regulamentar estes dispositivos móveis pertencentes a uma WLAN, foi criado um aparato de especificações pelo décimo primeiro (11) comitê de padronização IEE LAN/MAN (802).

IEEE não testa equipamentos, este trabalho é desenvolvido pelo grupo comercial Wi-Fi Alliance

JAMMING E INTERFERÊNCIA

Quando acidentalmente dificultamos a comunicação de um receptor, temos uma interferência. Já uma interferência proposital, se caracteriza um Jamming.

Forno de microondas.

- 2.45GHz;
- Dielectric;
- Antes do WiFi.

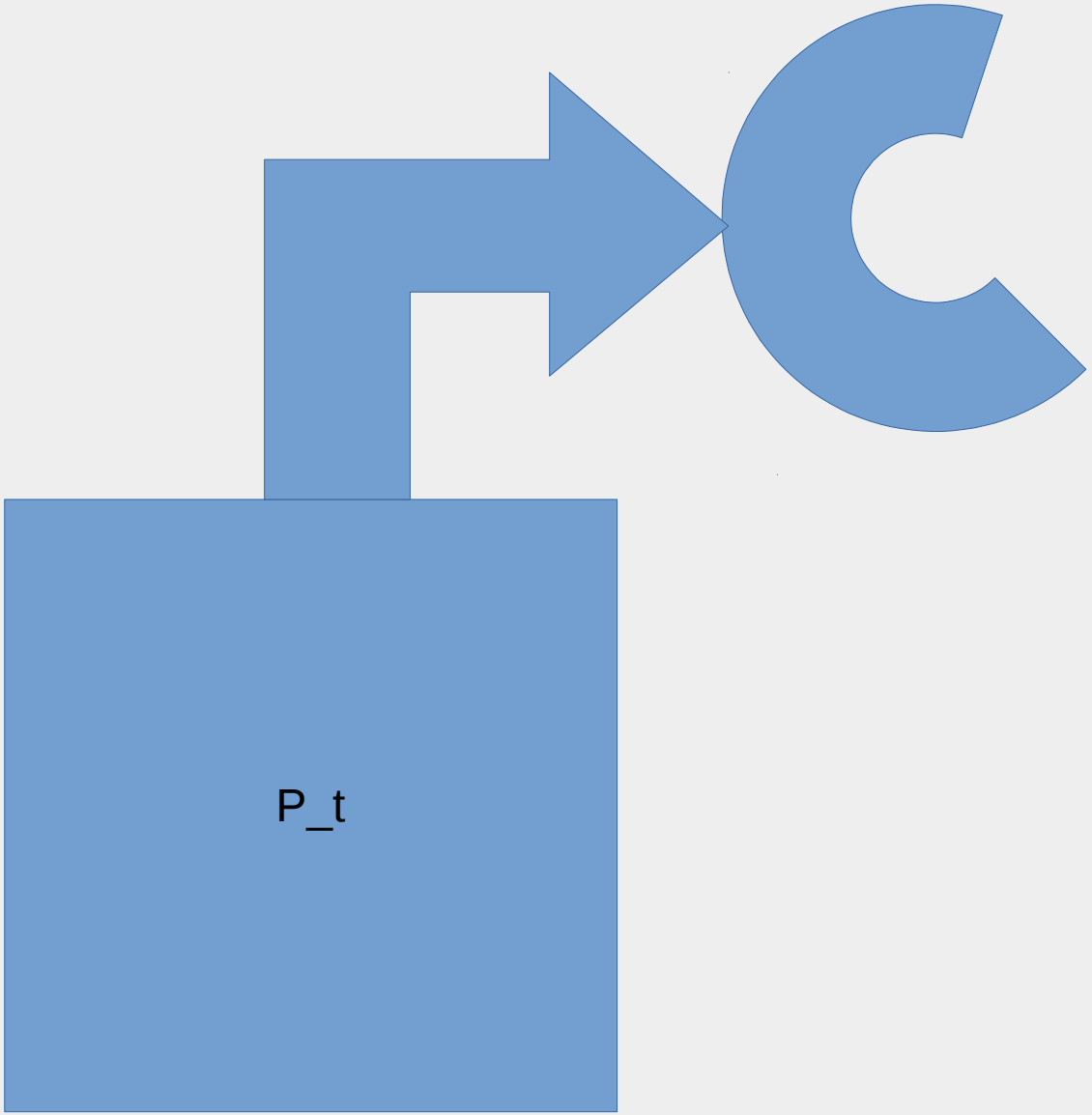
JAMMER / DDOS

- Camada 1
  - Transmissor RF.
- Camada 2
  - Deauthentication.

EIRP (POTÊNCIA EFETIVA TRANSMITIDA)

The EIRP can be related to the power transmitted from the radio (P_t), the cable losses (possibly including antenna mismatch) L, and the antenna gain (G) by:

$$EIRP = P_t - L + G$$


P_t

A resolução número 506 da Anatel, de 1º de julho de 2008, seção IX, artigo 39, capítulo 2, determina: “As condições estabelecidas nesta Seção, para a faixa 2.400-2.483,5 MHz, **não valem para os equipamentos cujas estações utilizem potência e.i.r.p. superior a 400 mW, em localidades com população superior a 500.000 habitantes.**”Neste caso, as estações deverão ser licenciadas na Agência, nos termos da regulamentação específica pertinente a esta faixa.

REMEDIAL ECCM TECHNIQUES

COMMUNICATIONS TECHNIQUES: ELECTRONIC COUNTER-COUNTERMEASURES (ECCM), descreve técnicas de proteção contra interferências inimigas no campo de batalha.

Tal documento define que os jammers operam contra receptores de duas formas, Spot e Barrage.

Spot é um ataque direcionado a um determinado canal ou frequência. Já o tipo Barrage, se propaga em várias portadoras ou frequências ao mesmo tempo.

Por mais que tais técnicas sejam direcionadas a receptores de rádio utilizados pelo exército em batalha, este documento serve como um guia de boas práticas de reconhecimento e combate a Jamming em redes WLAN, em conjunto com o guia ECCM.

JAMMER 2.600 Hz

NE555

Input:		
Frequency	0.00260	(KHz)
Duty Cycle	100	(%) ☑ Invert Output
RA	5.54	(KOhm)
RB	0.00	(KOhm)
C	100	(uF)
	Compute	

Equations:

F=1/T= 1.44/((RA+RB*2)*C)

TL= 0.693*RB*C

TH= 0.693*(RA+RB)*C

D= Duty Cycle= (RA+RB)/(RA+2*RB)

Or,

RA= 1.44**(2*D-1)/(F*C)

RB= 1.44*(1-D)/(F*C)

BLOQUEADORES DE SINAIS

O regulamento sobre equipamentos de radiocomunicação de radiação restrita, anexado a resolução número 506 da Anatel, determina que um **bloqueador de sinais de radiocomunicações (BSR)**, é um equipamento destinado a restringir o emprego de radiofrequências ou faixas de radiofrequências específicas para fins de comunicações.

PLATAFORMA BRASILEIRA DE BLOQUEIO DE SINAIS DE RADIOCOMUNICAÇÕES

PLATAFORMA BRASILEIRA DE BLOQUEIO DE SINAIS DE RADIOCOMUNICAÇÕES, termina as características técnicas básicas para frequências de 870,0 MHz – 2170,0 MHz, com potência máxima de saída de 15.5(W), ou 40.96 dBm.

BLOQUEADORES DE SINAIS 2.4GHz EDUCACIONAIS

Este, como já se era de esperar, não é o único trabalho que aborda o conceito de Jammer em banda ISM. No entanto, um dos diferenciais deste documento, é a objetividade de por em prática e em teste, as aplicabilidades de interferências propositais em dispositivos Wlan.

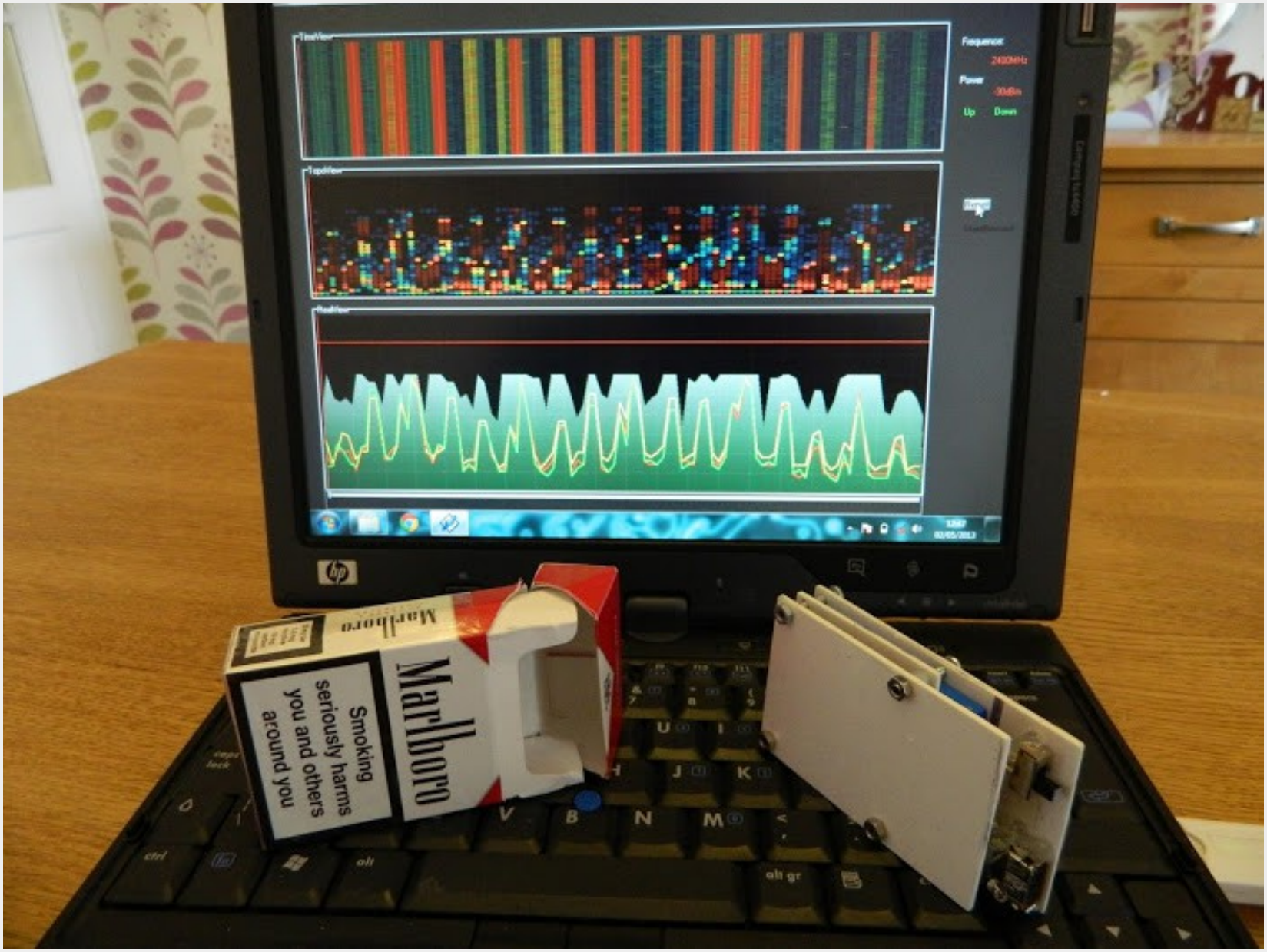
WHAT WOULD MACGYVER DO ?

http://wwmgd.blogspot.com.br/


Next firmly tape down
all the number buttons

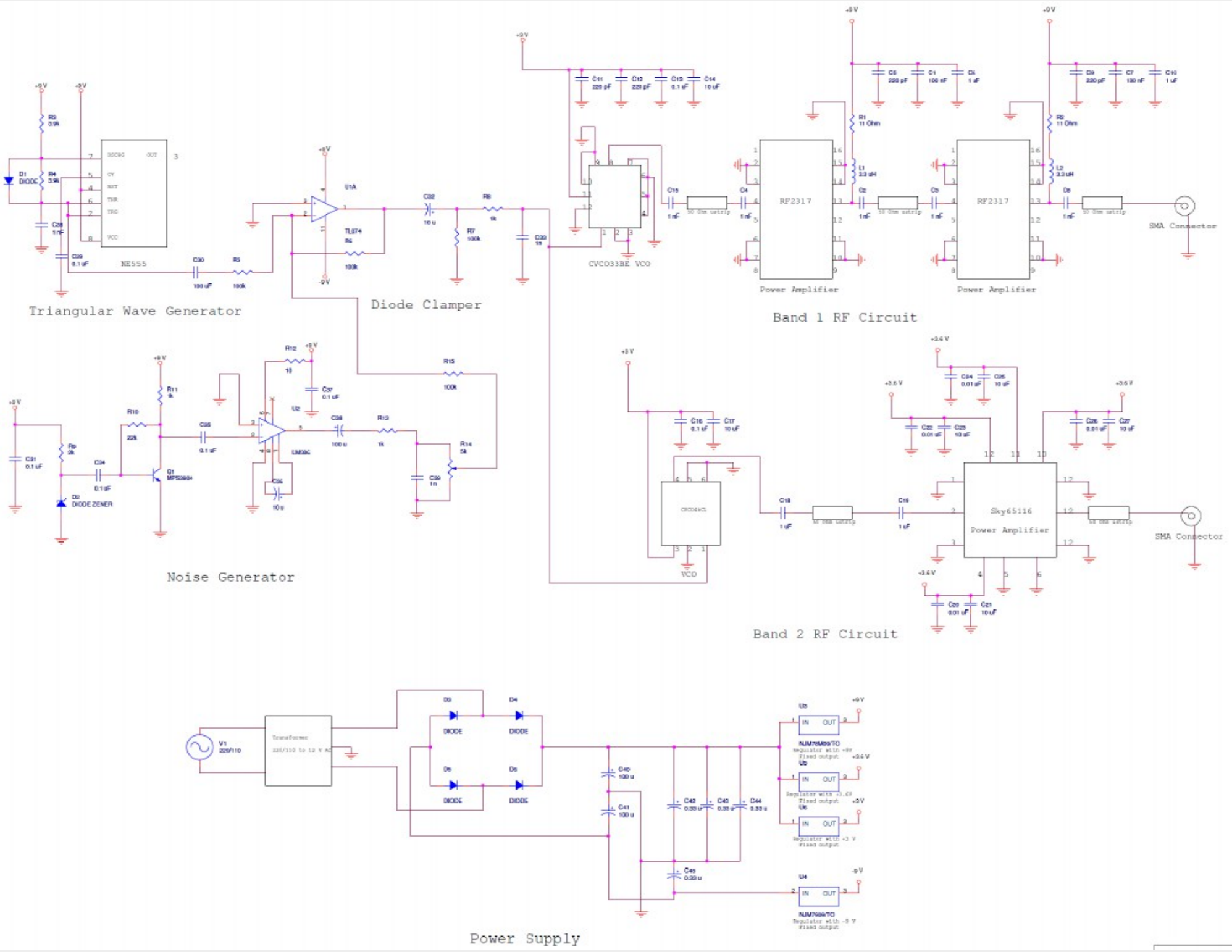
BUILD YOUR OWN WIFI JAMMER

Andrew Mcneil's


Frequency
Power
Up
Down
Marlboro
Smoking seriously harms you and others around you
Marlboro

DRONE JAMMER

Ahmad Jisrawi

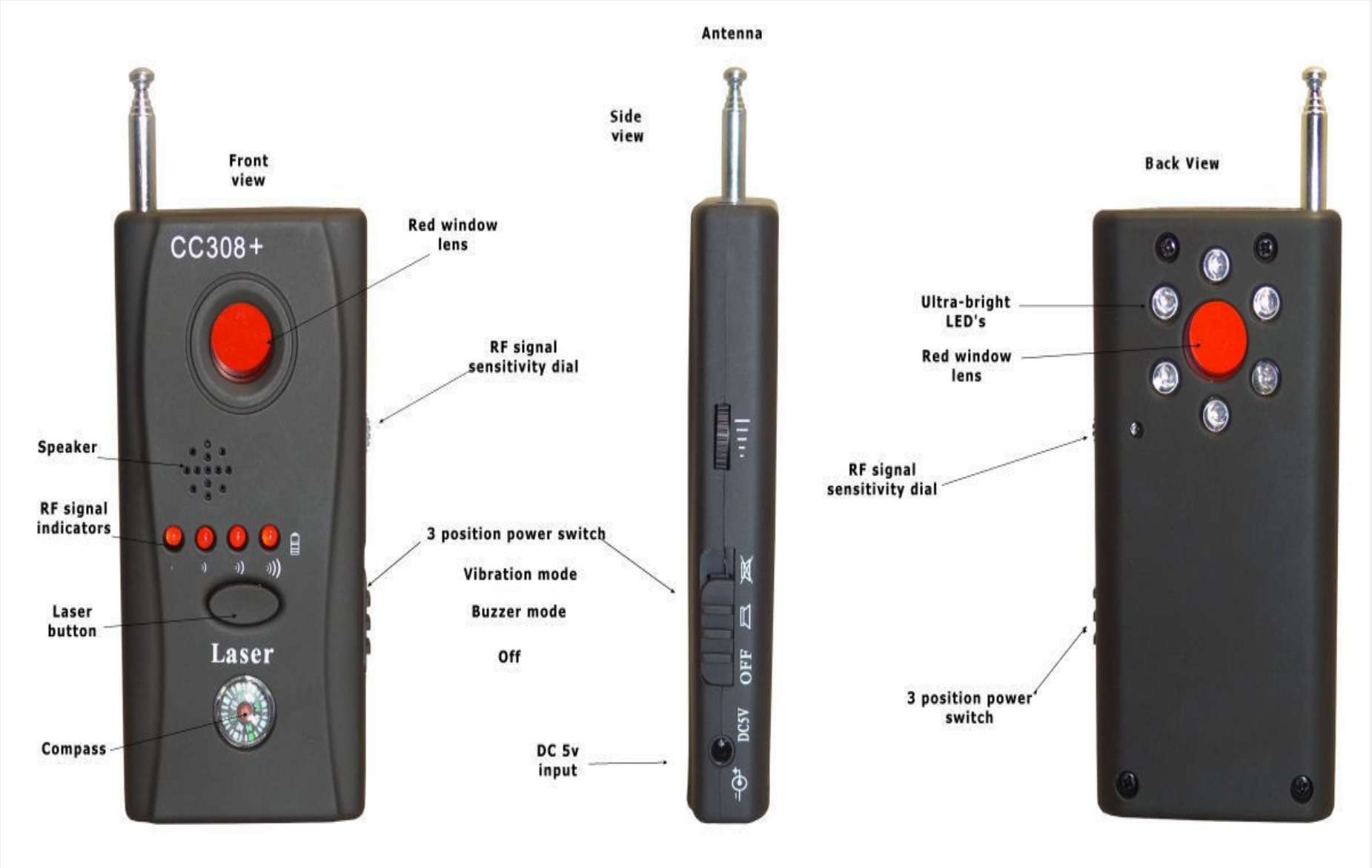

NE555
Triangular Wave Generator
Diode Clamper
CVCO33BE VCO
RF2317
Power Amplifier
RF2317
Power Amplifier
SMA Connector
Band 1 RF Circuit
Noise Generator
VCO
Sky65116
Power Amplifier
SMA Connector
Band 2 RF Circuit
Transformer
DIODE
DIODE
DIODE
DIODE
Power Supply

BUG DETECTOR

Detectores de rádio frequência são usados para monitorar a voltagem de saída emitida por sistemas sem fio. A energia RF é a principal medida de um sinal sem fio. Em um transmissor, ele representa a quantidade de energia que é emitida e deverá respeitar normas e limites.

Detectores de sinais para uso pessoal, são fáceis de manusear e tem preço acessível, ao contrário dos complexos aparelhos de medição profissional de sinais, que além de terem preços elevados, requerem mão de obra qualificada para operá-los.

CC308+

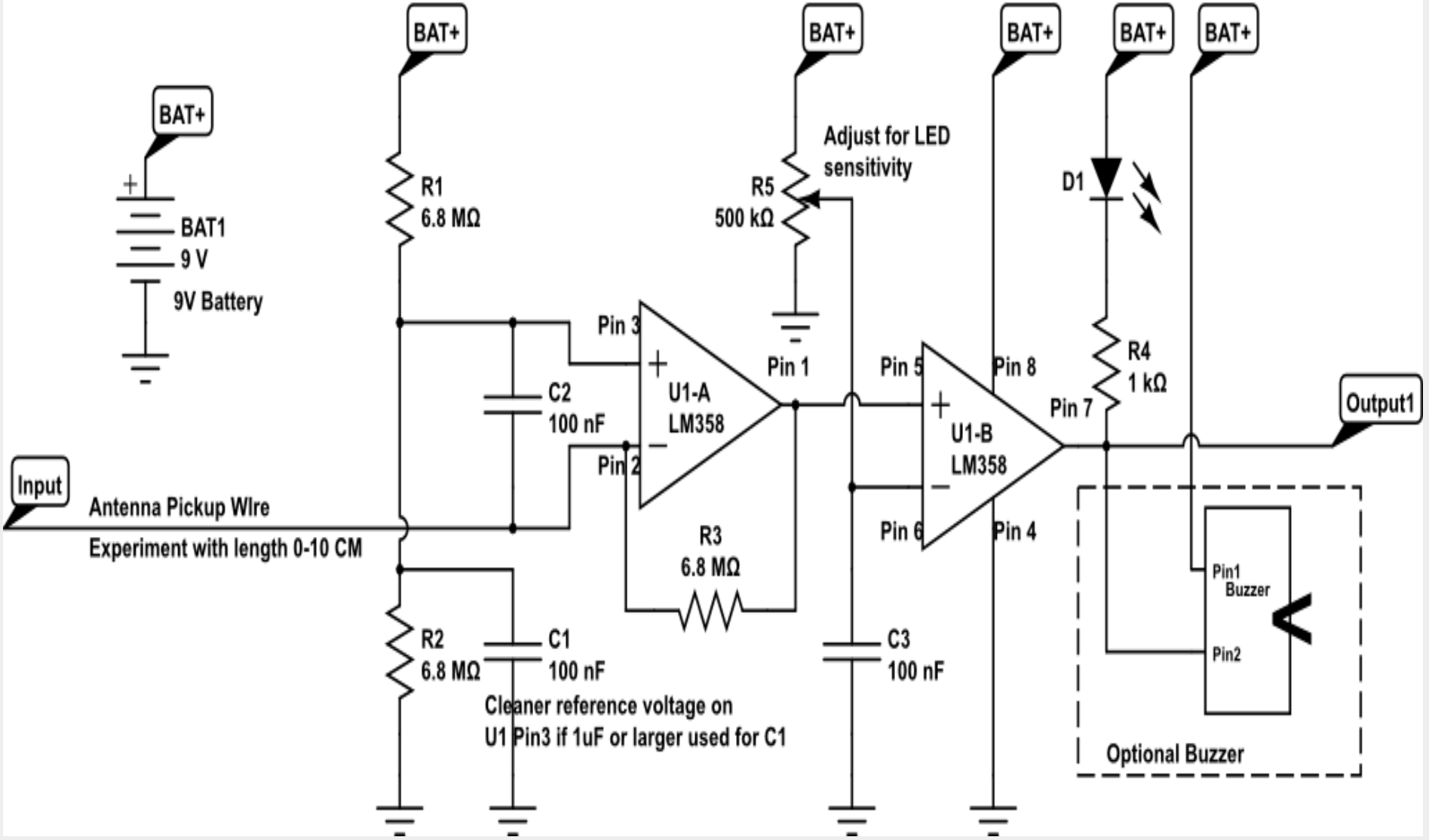

Front view
CC308+
Red window lens
RF signal sensitivity dial
Speaker
RF signal indicators
3 position power switch
Vibration mode
Buzzer mode
Off
Laser button
Laser
Compass
DC 5v input
Antenna
Side view
OFF
DC5V
Back View
Ultra-bright LED's
Red window lens
RF signal sensitivity dial
3 position power switch

Cell phone detector

Cell Phone Detector

Revision: 10-10-2012

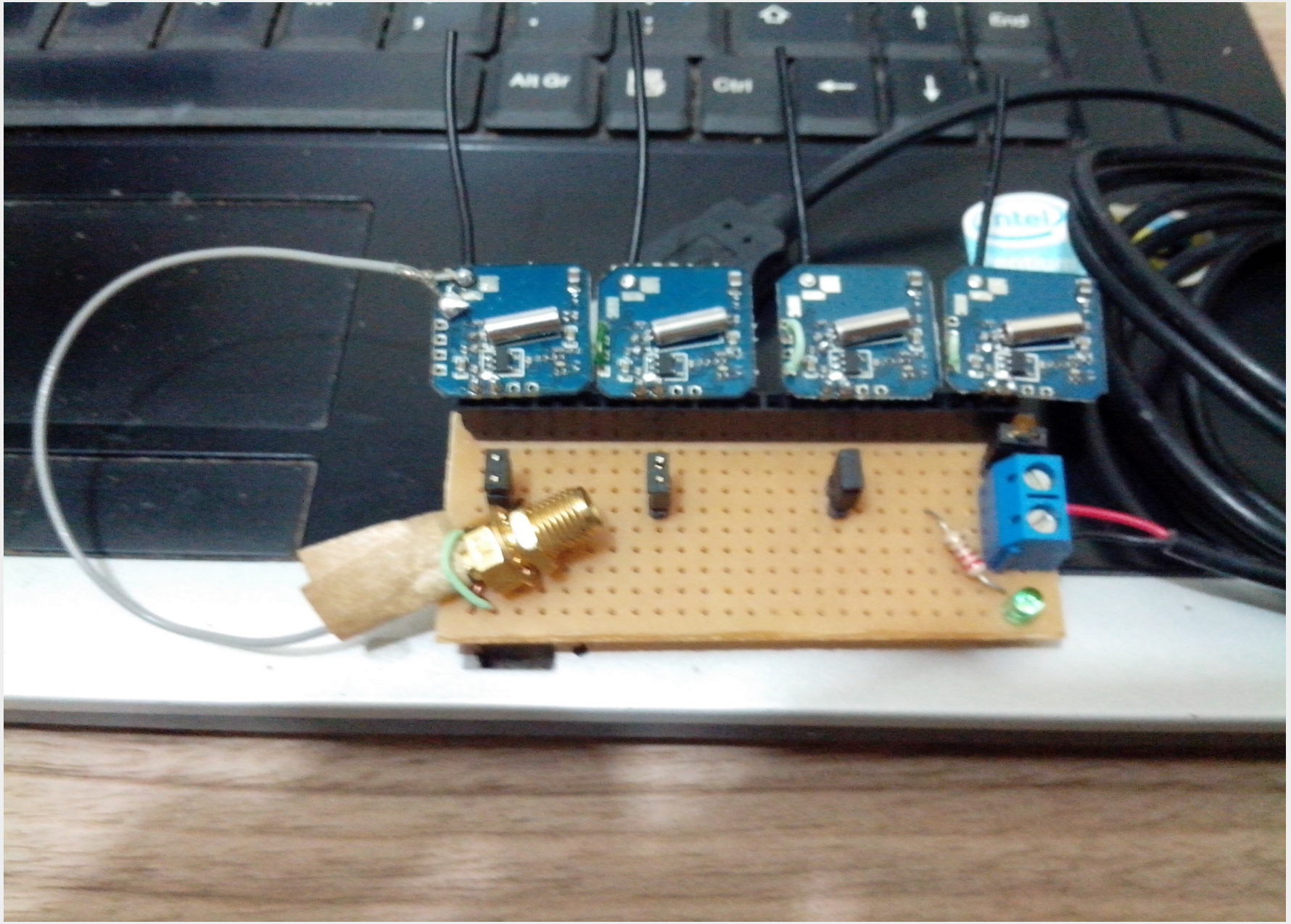
The LM358 is a single supply dual OpAmp in a 8 pin package.



O HARDWARE

De simples montagem, aproveitando as características RF do arranjo de quatro 4 transmissores de áudio e vídeo, modelo XL24017, que operam na banda ISM, nas frequências 2.414GHz a 2.468 GHz.


SEMP TOSHIBA info
STi
Legrand
Legrand
EXPEC®
cloridrato de oxomemazina (2mg/5ml) +
iodeto de potássio (100mg/5ml) +
benzoato de sódio (20mg/5ml) +
guaifenesina (30mg/5ml)
NÃO CONTÉM AÇÚCAR
EXPECTORANTE
ANTIALÉRGICO
ANTITUSSÍGENO
ANTI WIFI
SABOR FRAMBOESA E CARAMELO
USO ADULTO
E PEDIÁTRICO
USO ORAL
120 ml
CONTEÚDO
XAROPE

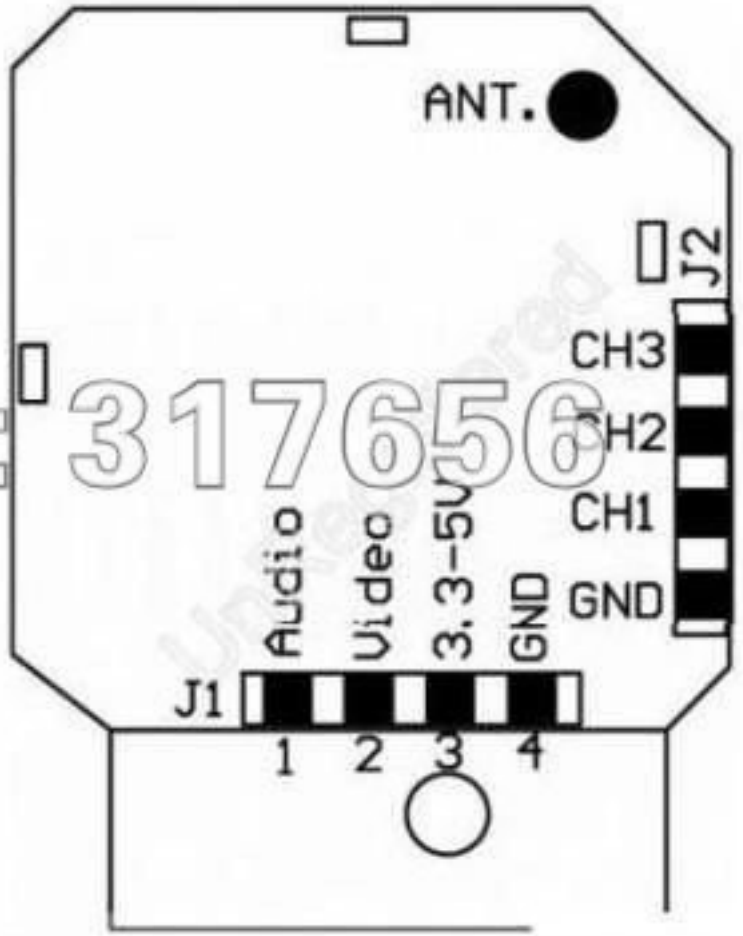

Alt Gr
Ctrl
End

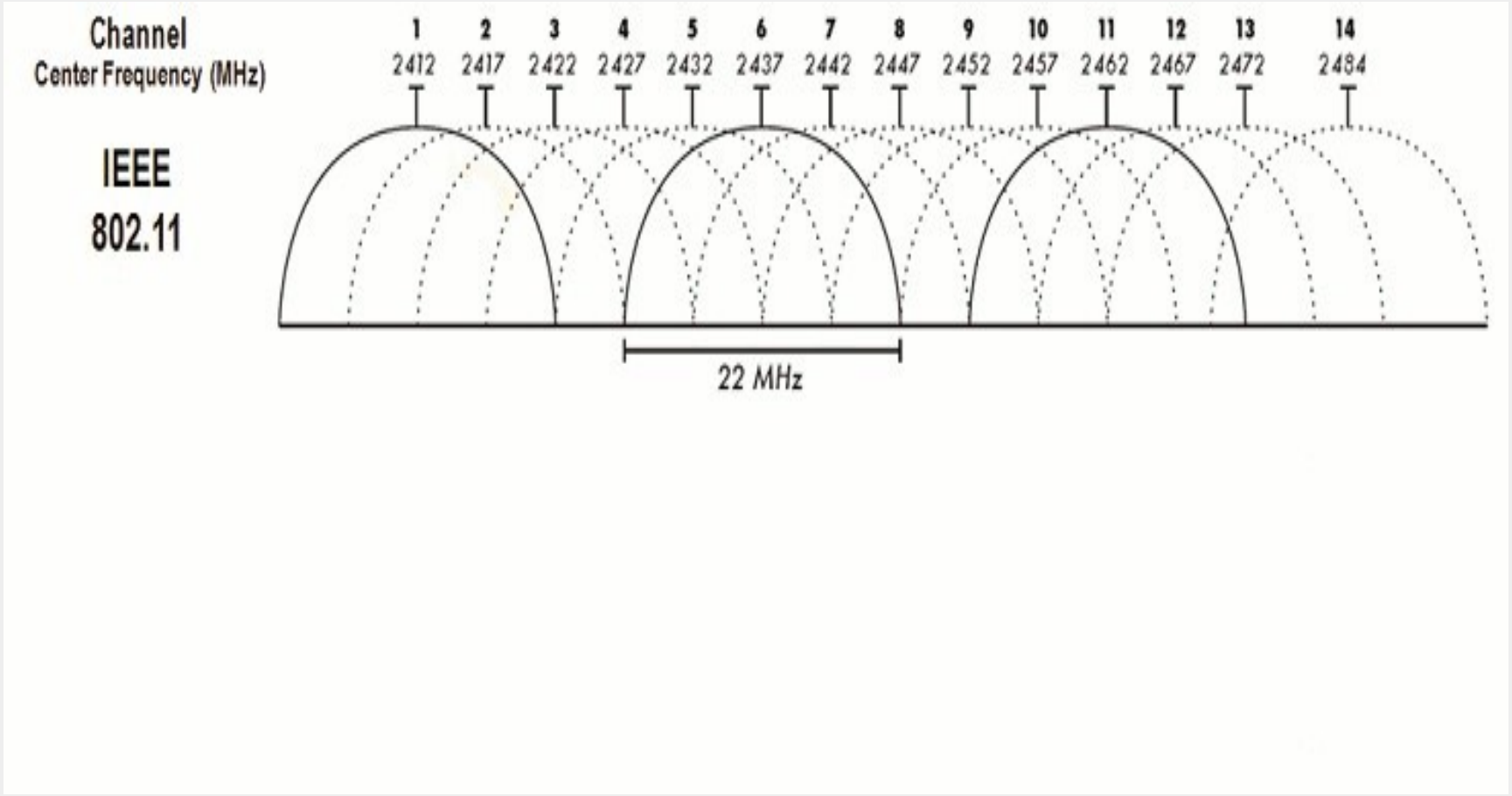
XL24017

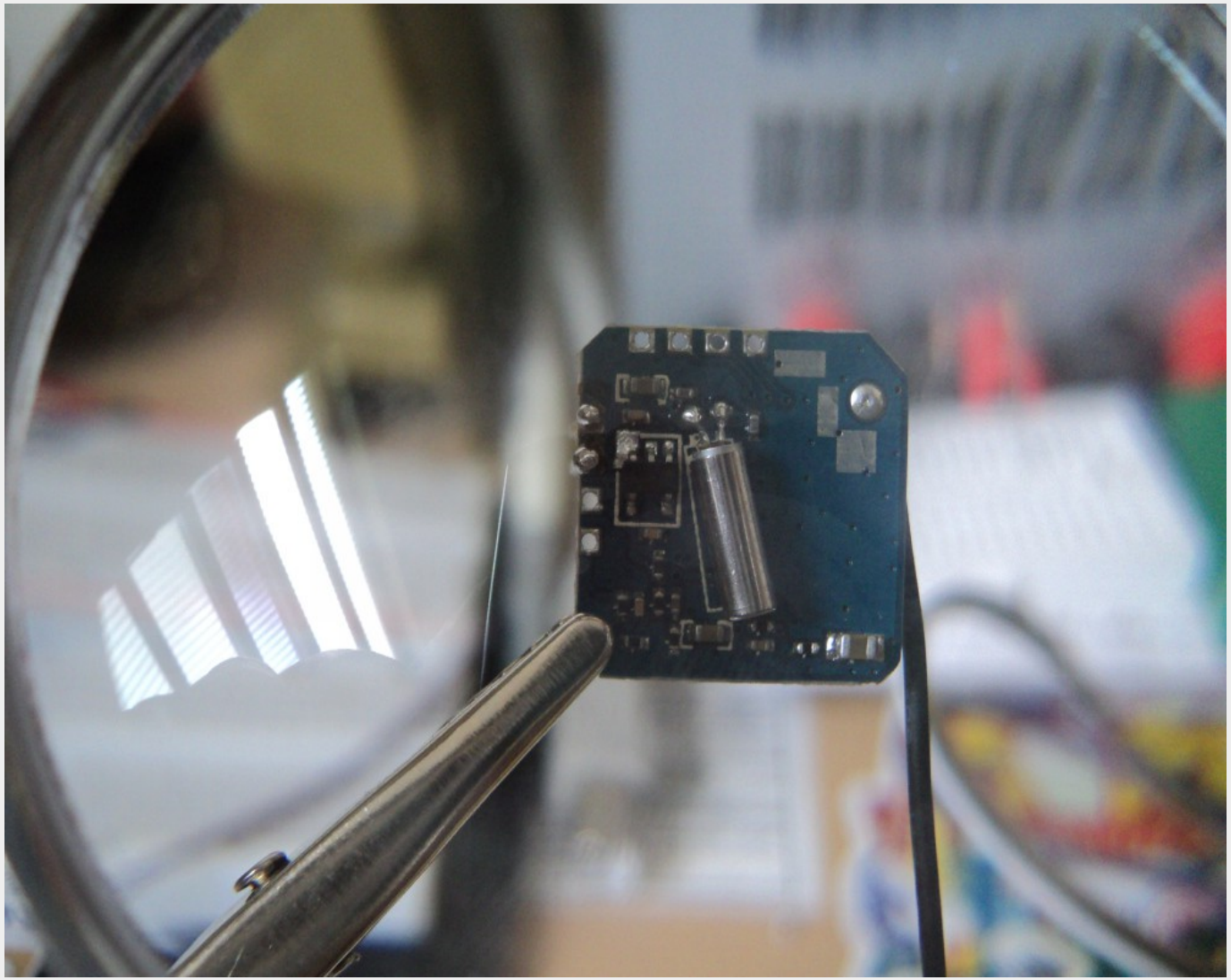
6 引脚分布（Pin Assignment ）

J1 Pin No.	Function
1	Audio
2	Video
3	Vcc(DC+5V)
4	GND

J2 Pin No.	Function
1	GND
2	CH1：2.414GHz
3	CH2：2.432GHz
4	CH3：2.450GHz




Channel
Center Frequency (MHz)
IEEE
802.11
1 2412
2 2417
3 2422
4 2427
5 2432
6 2437
7 2442
8 2447
9 2452
10 2457
11 2462
12 2467
13 2472
14 2484
22 MHz

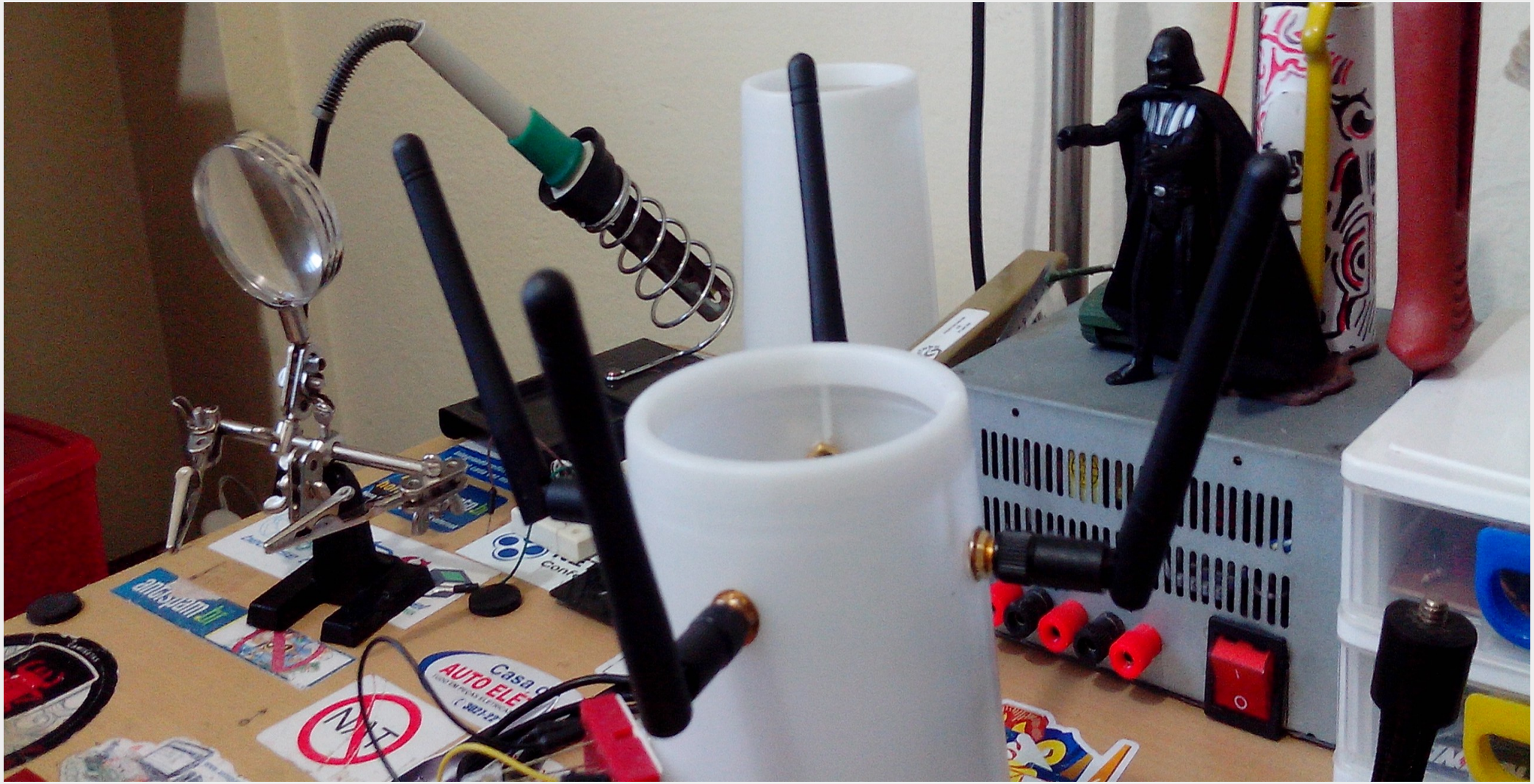


LISTA DE COMPONENTES

XL24017	4
ANTENA 2.2dBi / 2,4GHZ / 50 ohms	4
Pigtail 50 ohms	4
Placa de protótipo / 170 furos	1
Cabos tipo jumper	12
Led 5mm	1
Resistor 1k Ohm	1

AS ANTENAS

Para concentrar o sinal e aumentar a potência efetiva de transmissão, foram utilizadas quatro (4) antenas omnidirecionais, uma para cada transmissor.


AUTO

ROGUE AP

Quando, de forma indevida, um ponto de acesso sem fio é estabelecido em um ambiente corporativo, no intuito de criar um backdoor de acesso a rede privada, temos um roguer ap.

CENÁRIO

- Uso de um software ap.

JAMMER NO CENÁRIO II

- Anular com o Jammer

SEGURANÇA DE PERÍMETRO


Here's
Mr. Jones
in 2020…
Replacement hip
medical part #459382
Wig
model #4456
(cheap polyester)
Das Kapital and
Communist-
party handbook
1500 Euros
in wallet
Serial numbers:
597387,389473
…
30 items
of lingerie

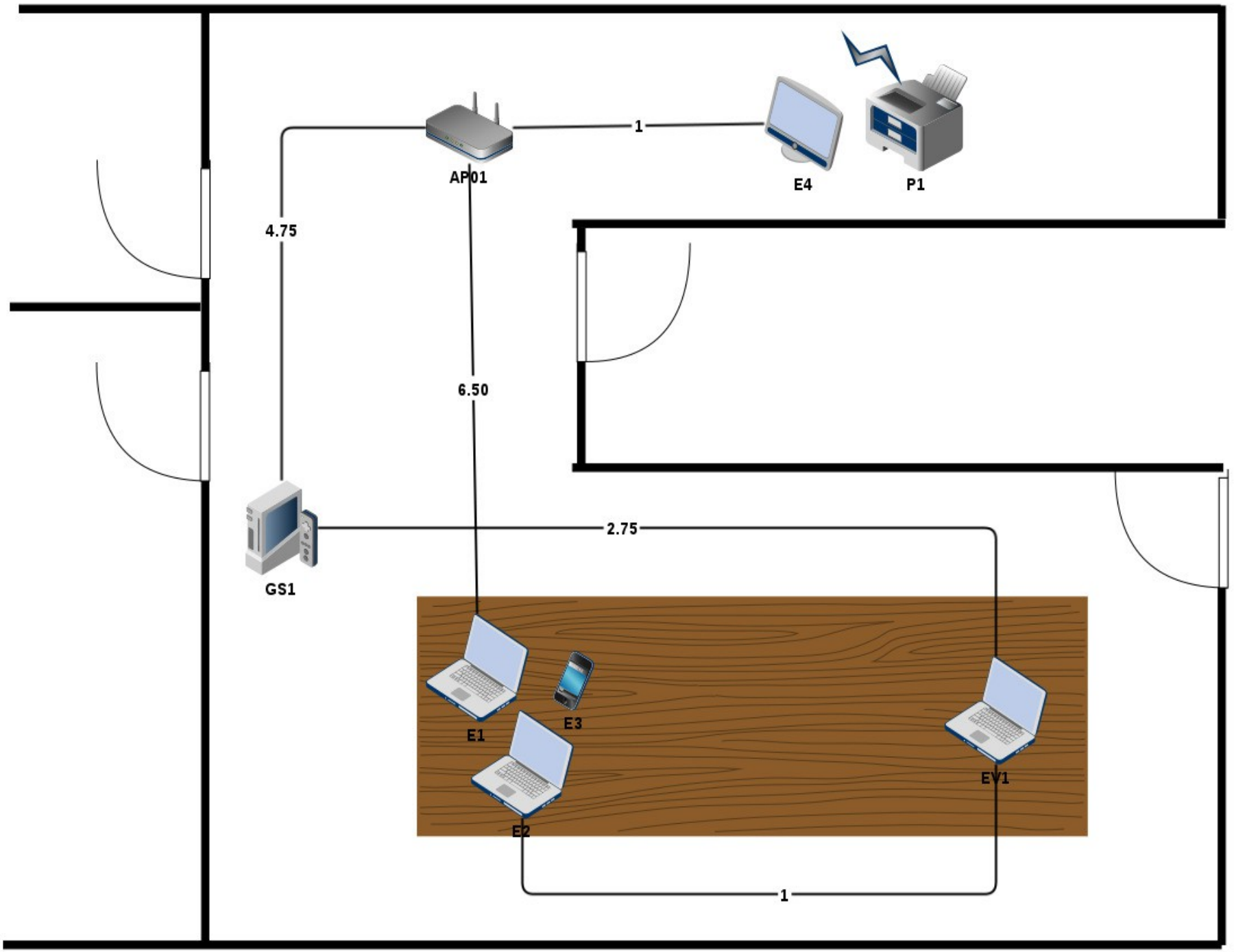
EVIL TWIN

Diferente do ataque roguer ap, um ataque do tipo evil twin, não é causado acidentalmente. Nesta variação de ataques maliciosos a equipamentos Wifi, um criminoso tem plena consciência dos seus atos.

Pacotes de gerenciamento 802.11 são fáceis de injetar maliciosamente numa rede Wifi.


AP1

AP PHISHING COM DEAUTHENTICATION E JAMMER


AP01
1
E4
P1
4.75
6.50
2.75
GS1
E1
E3
E2
EV1
1

CARACTERÍSTICAS DE CADA COMPONENTE

EV1 Notebook Gnu Linux (Slackware) ,Wireless Card: AR9285 – 20dBm – 100mW
AP01 Access Point LuCI Firmware (OpenWrt) , E.R.I.P: 26 dBm – 400mW
E1 Notebook Gnu Linux (Slackware), Wireless Card: – 20dBm – 100mW
E2 Notebook Ms Windows (7), Wireless Card: – 20dBm – 100mW
E3 Celular Android (4.1.2) , Motorola Rzor D1
E4 All-in-one Slackware Wireless Card: RTL8188CE 802.11b/g/n WiFi Adapter – 20dBm – 100mW
GS1 Console de jogos Xbox Operating System Internal Wireless N WIFI Internet Card OEM Genuine Model 1400
P1 Impressora Epson Firmware Modelo XP-214
EAP Access Point Epson Firmware WRTR-141
200 mW

EVIL TWIN COM **DEAUTHENTICATION** – SOFTWARE AP – NO MESMO CANAL DE AP01 (CH-1) – SSID JAMMER – (AIRPLAY-NG, AIRBASE-NG)

Vídeo

EVIL TWIN COM **JAMMER** – SOFTWARE AP E HARDWARE AP – NO MESMO CANAL DE AP01 (CH-1) – SSID JAMMER – (AIRBASE-NG)

Este tipo de ataque passa a usar o jammer como forma de desassociação dos alvos conectados em AP01. Após um mapeamento de canais e identificadores, EV1 configura o jammer para gerar ruídos no canal do ponto de acesso alvo e cria um ponto falso com o mesmo canal. Neste caso, as chances de sucesso são quase nulas, já que o canal está inutilizável por causa do efeito da interferência criada pelo jammer.

EVIL TWIN COM **JAMMER** – *SOFTWARE AP* –
CH 11 – SSID JAMMER – (AIRBASE-NG)

E2 (Ms Windows) foi a única a cair no evil twin.

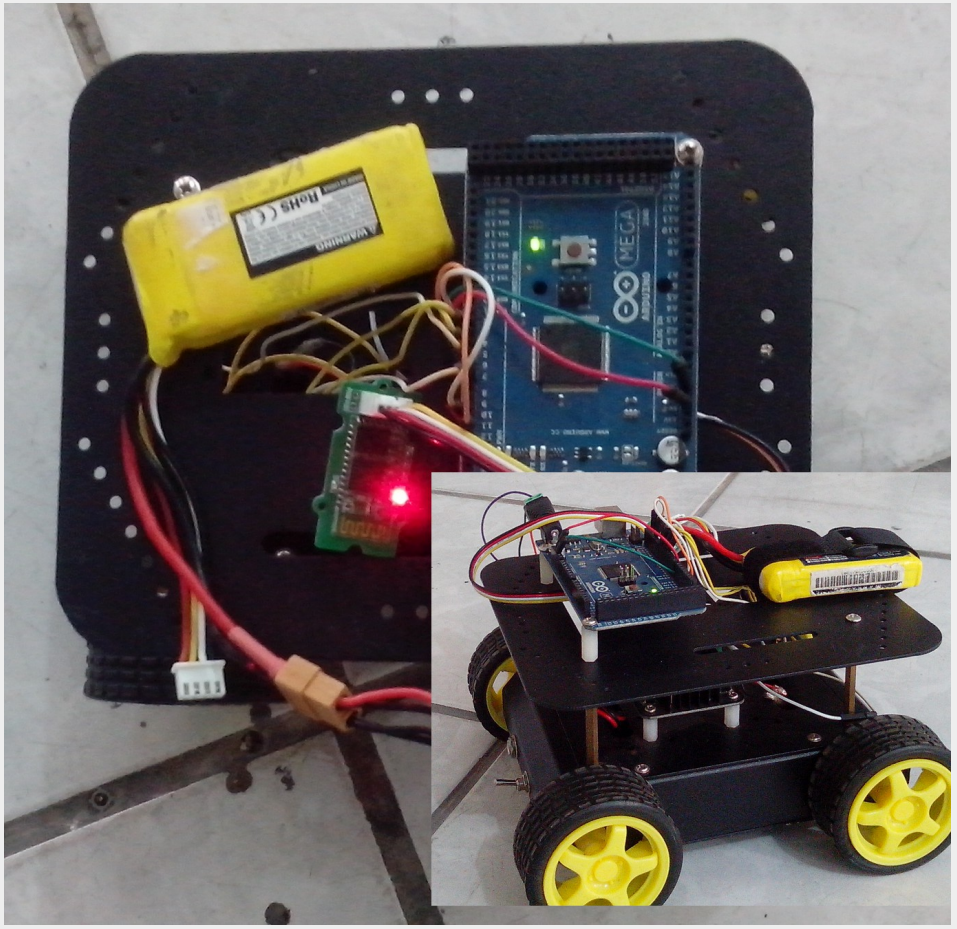
Vídeo

EVIL TWIN COM **JAMMER** – *HARDWARE AP* – CH 11 – SSID JAMMER

EAP proporcionou melhores resultados para este tópico. Em teste anterior, utilizando software ap, **apenas E2 foi enganado**. Na simulação com hardware, mais uma vez E2 é redirecionado entre pontos de acesso. GS01, por sua vez, também foi redirecionado para EAP. Assim como E3, que saiu de AP01 para EAP, mas não renovou o endereçamento IP.

BLUETOOTH

ROBOTS JAMMER



Obrigado.