Sensorless, Permissionless Information Exfiltration with Wi-Fi Micro-Jamming

ROM OGEN (ROMOG@POST.BGU.AC.IL)

OMER SHWARTZ (OMERSHV@POST.BGU.AC.IL)

KFIR ZVI (ZVIKF@POST.BGU.AC.IL)

YOSSI OREN (YOS@BGU.AC.IL)

BEN-GURION UNIVERSITY OF THE NEGEV, ISRAEL

CBG / CSRC

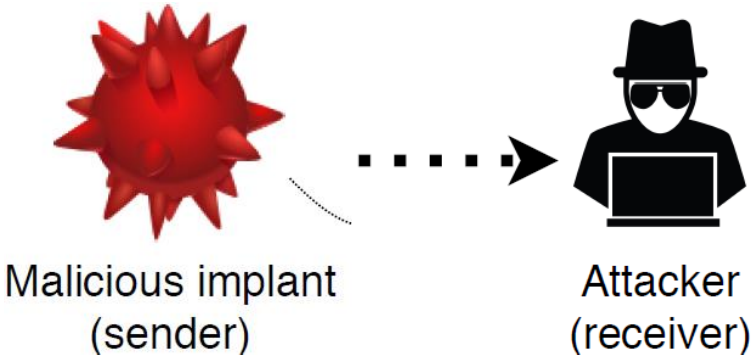
Cyber@Ben-Gurion
University of the Negev

Cyber Security
Research Center

Israel National
Cyber Bureau

Background

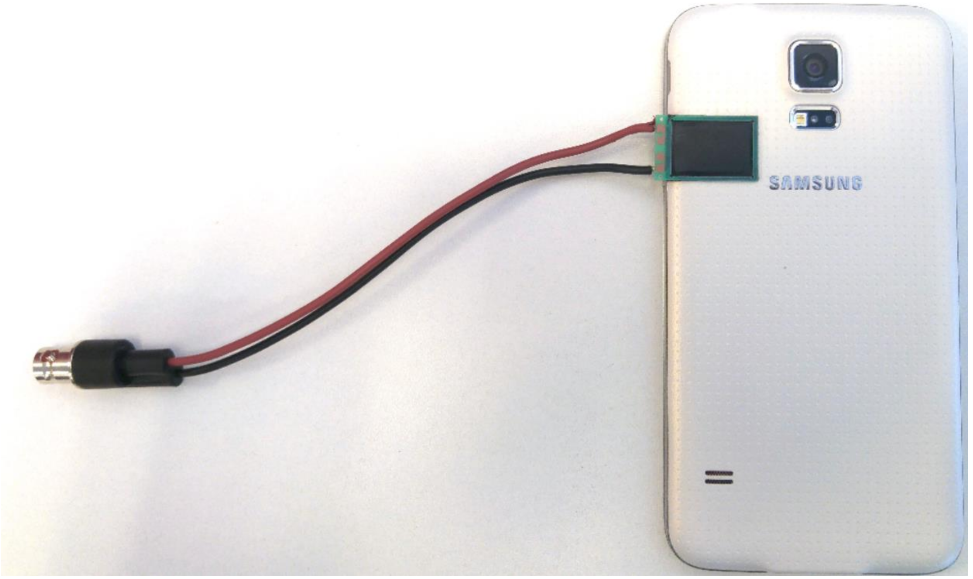
“A covert listening device, more commonly known as a bug or a wire, is usually a combination of a miniature **radio transmitter** with a microphone. The use of bugs, called bugging, is a common technique in surveillance, espionage and police investigations. “ - Wikipedia



Previous Works

Farshteindiker et al. [1] used a device’s gyroscope to exfiltrate data through a victim device.

A piezoelectric device causes interferences to the gyroscope sensor that are readable through a javascript running on the device.



[1] Farshteindiker, Benyamin, Nir Hasidim, Asaf Grosz, and Yossi Oren. "How to Phone Home with Someone Else's Phone: Information Exfiltration Using Intentional Sound Noise on Gyroscopic Sensors." In *WOOT*. 2016.

Objectives

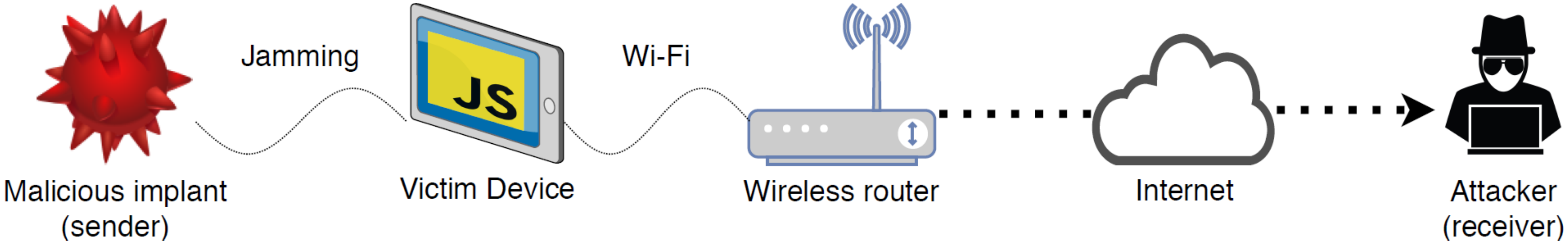
Develop and evaluate an exfiltration technique that maintains the advantages:

1. Covert
2. Permissionless
3. Long range

While reducing the limitations:

1. Need of physical contact with the victim
2. Power requirements

Our Contribution



"Covert channels through external interference."

Shah and Blaze [2] introduced the concept of an “interference channel”, which they defined as a “covert channel that works by creating external interference on a shared communications medium”

[2] Shah, Gaurav, and Matt Blaze. "Covert channels through external interference." *Proceedings of the 3rd USENIX conference on Offensive technologies (WOOT09)*. 2009.

Interference Channel

The sender cannot communicate directly with the receiver.

The victim is an uninvolved, unknowing device performing normal communications.

The receiver is capable of receiving some output from the victim and has the ability to separate the benign data from the payload.

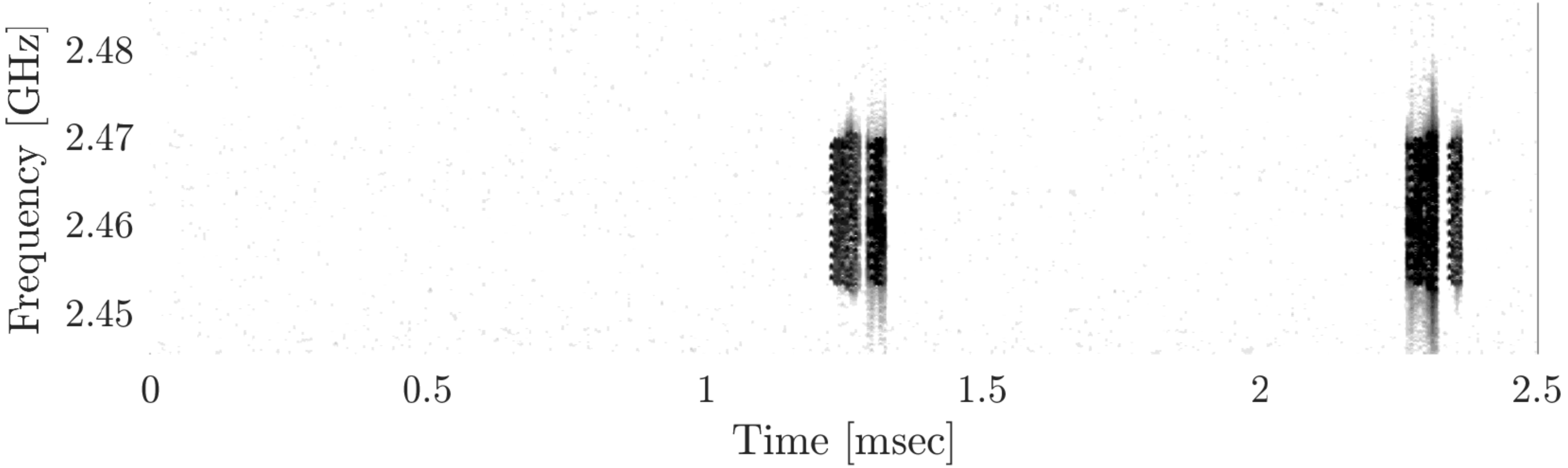
The malicious communication is hiding in plain sight.

Micro-Jamming

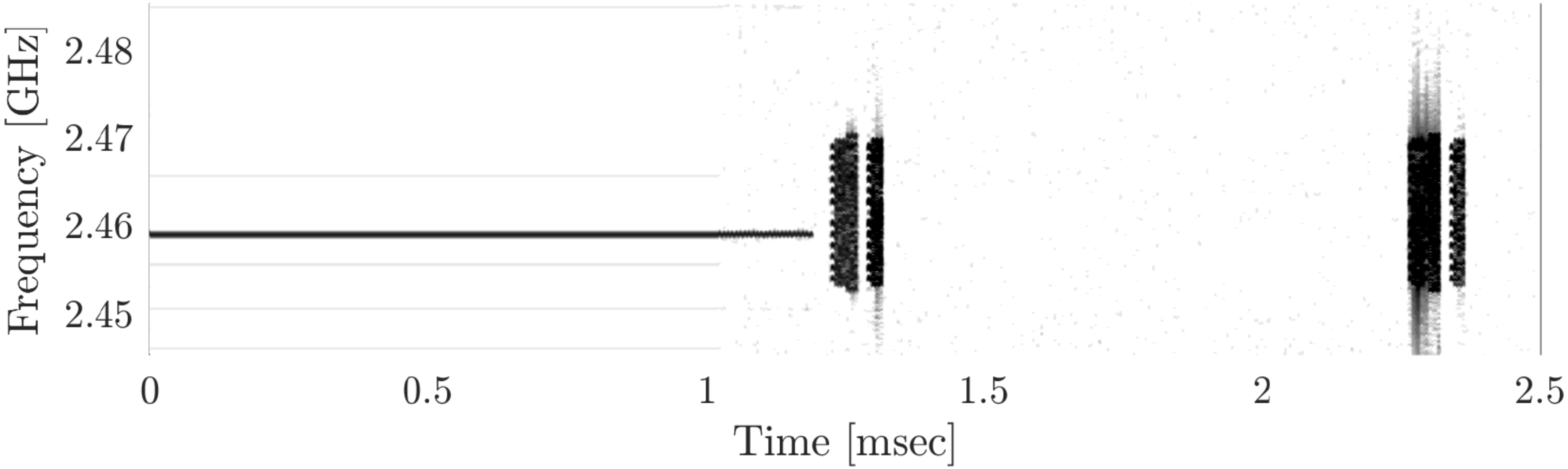
Many communication protocols, including 802.11, incorporate CCA (Clear Channel Assessment) mechanisms to maintain non-distruptiveness.

By briefly jamming the radio channel, Wi-Fi frames and responses can be delayed for several milliseconds.

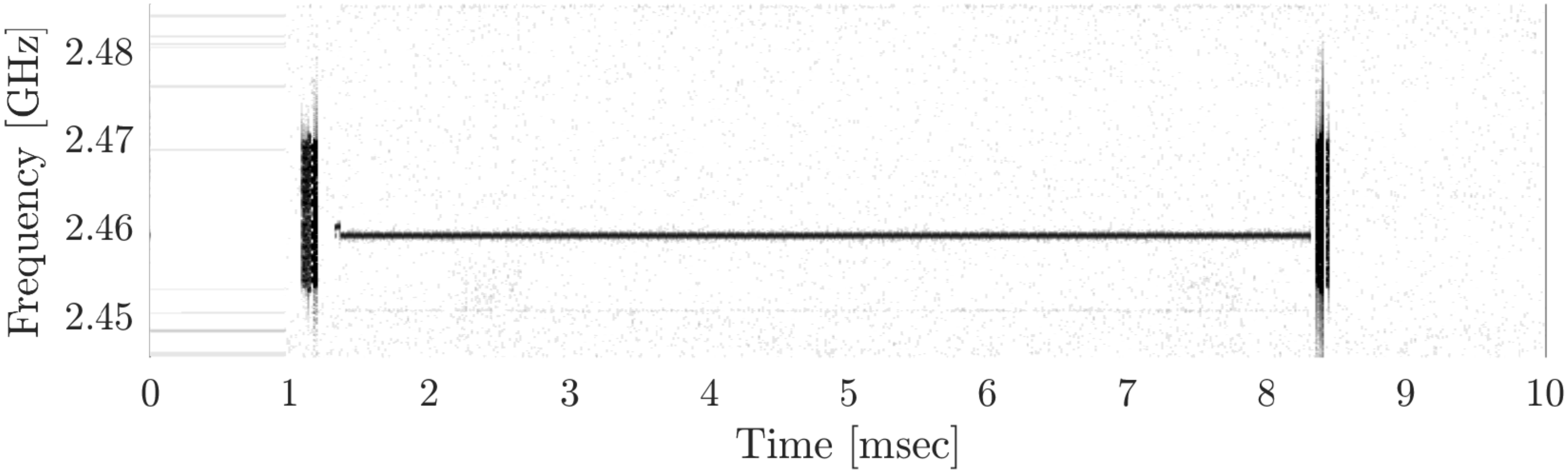
Micro-Jamming



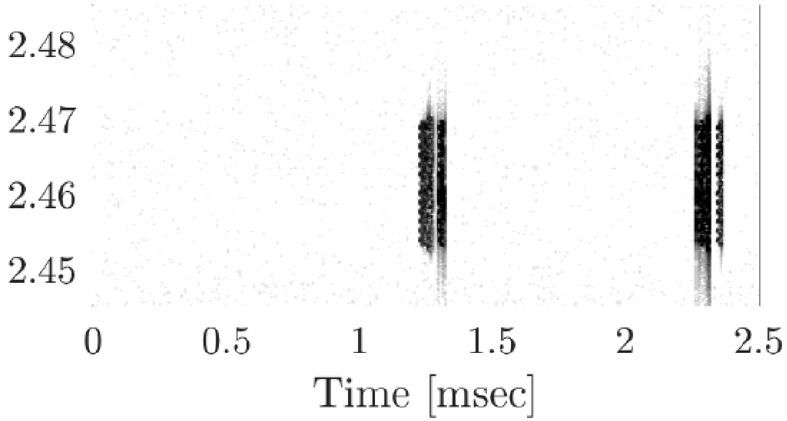
Micro-Jamming

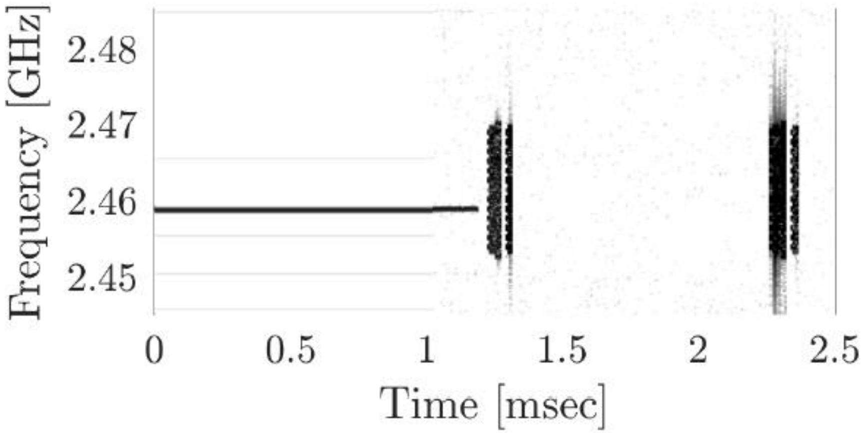


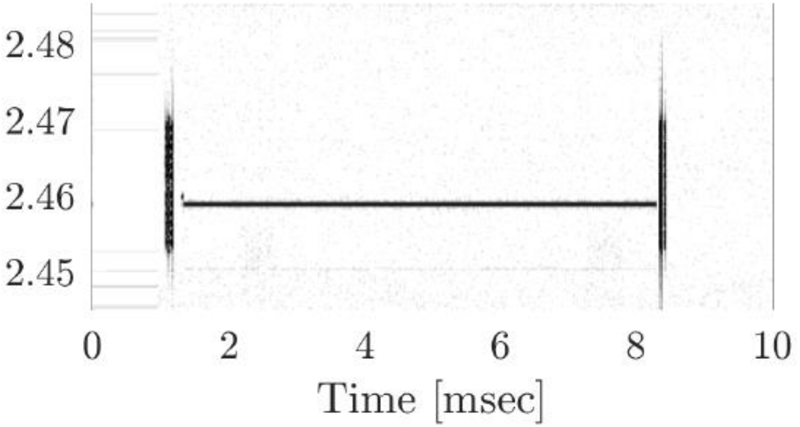
Micro-Jamming



Micro-Jamming



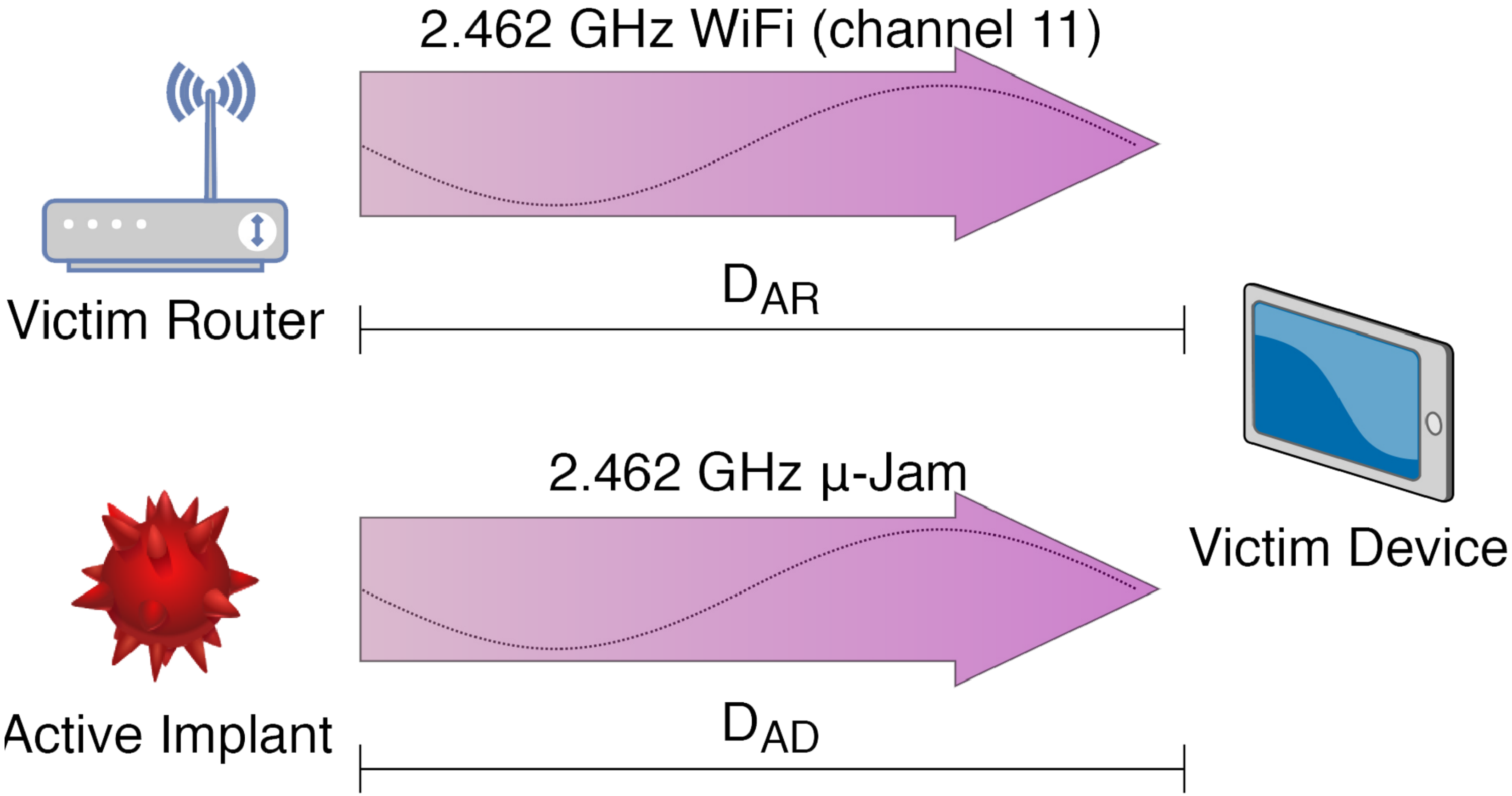




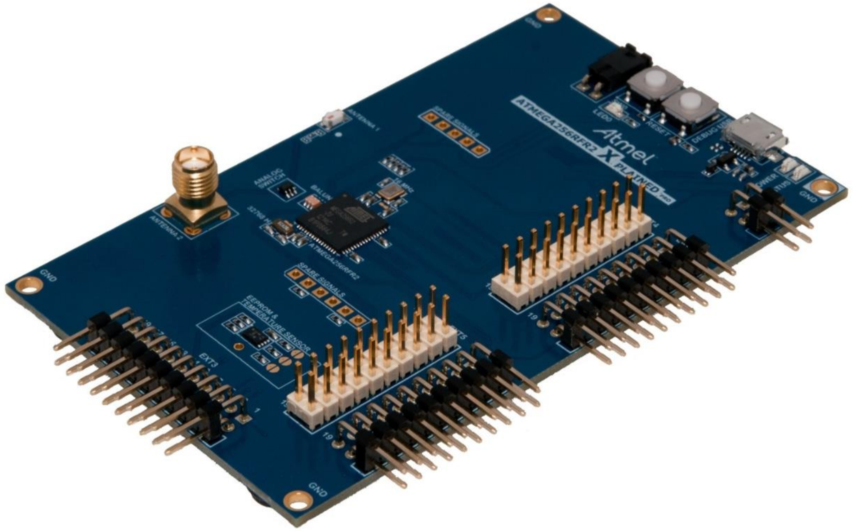
Traditional Jamming vs Micro-Jamming

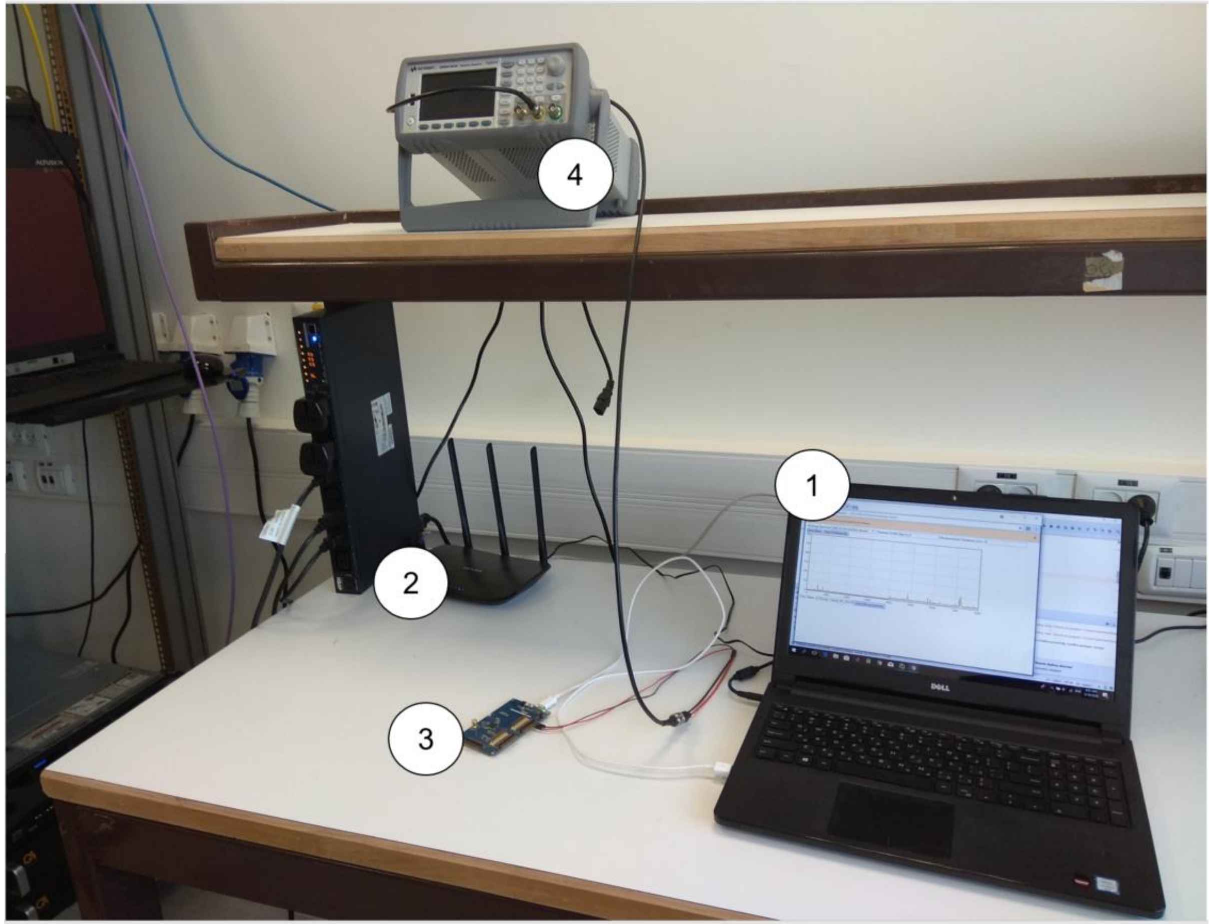
	Traditional Jamming	Micro-Jamming
Mode of operation	Packet loss	Packet delay
Network layers affected	At least 1-2	Only layer 1
Required transmission power	Stronger than blocked signal	Minimum required for sensing

Test Setup - Active



Test Setup - Active





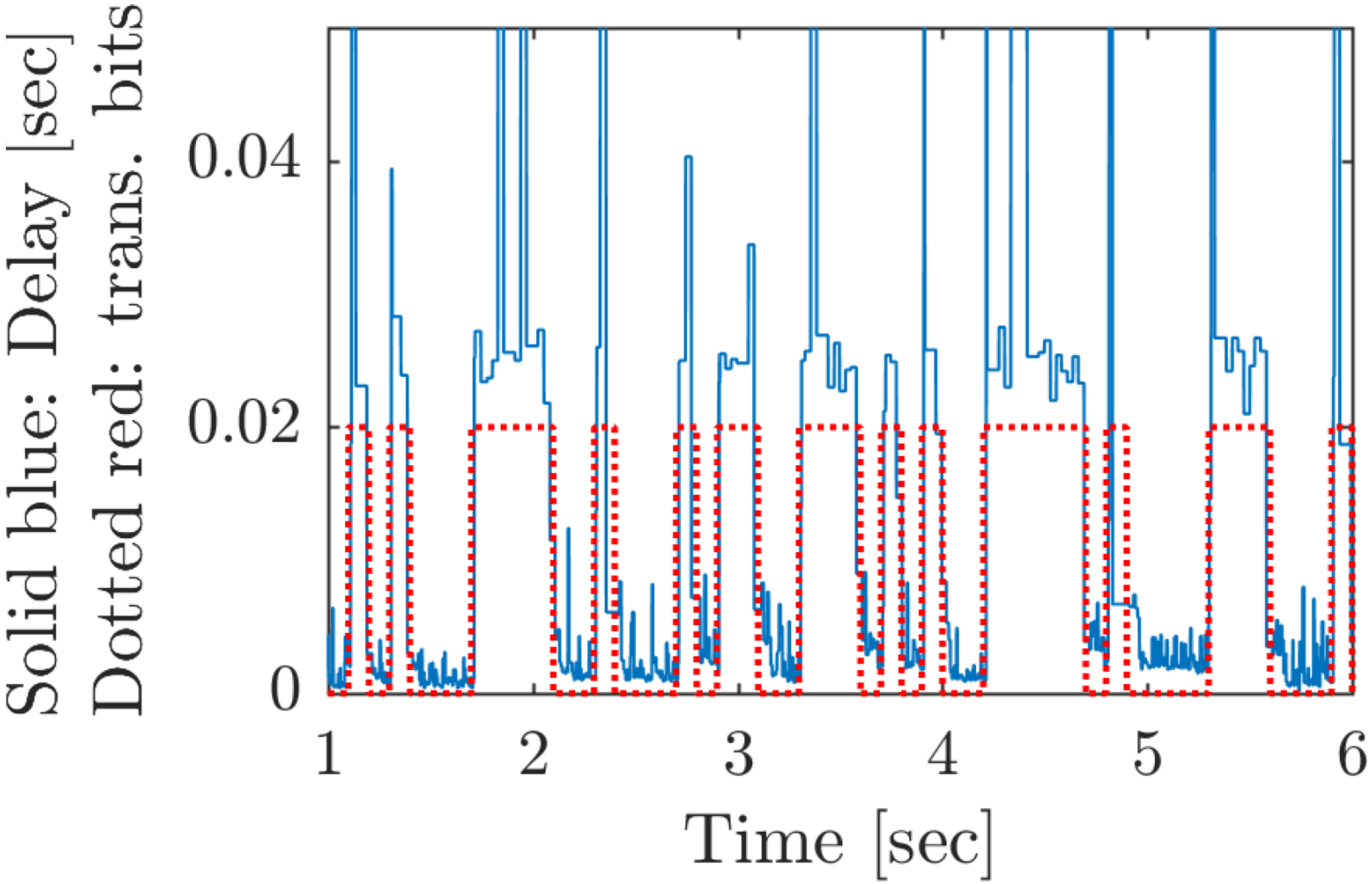
Test Setup - Active

ATMEGA256RFR2 Xplained Pro evaluation board

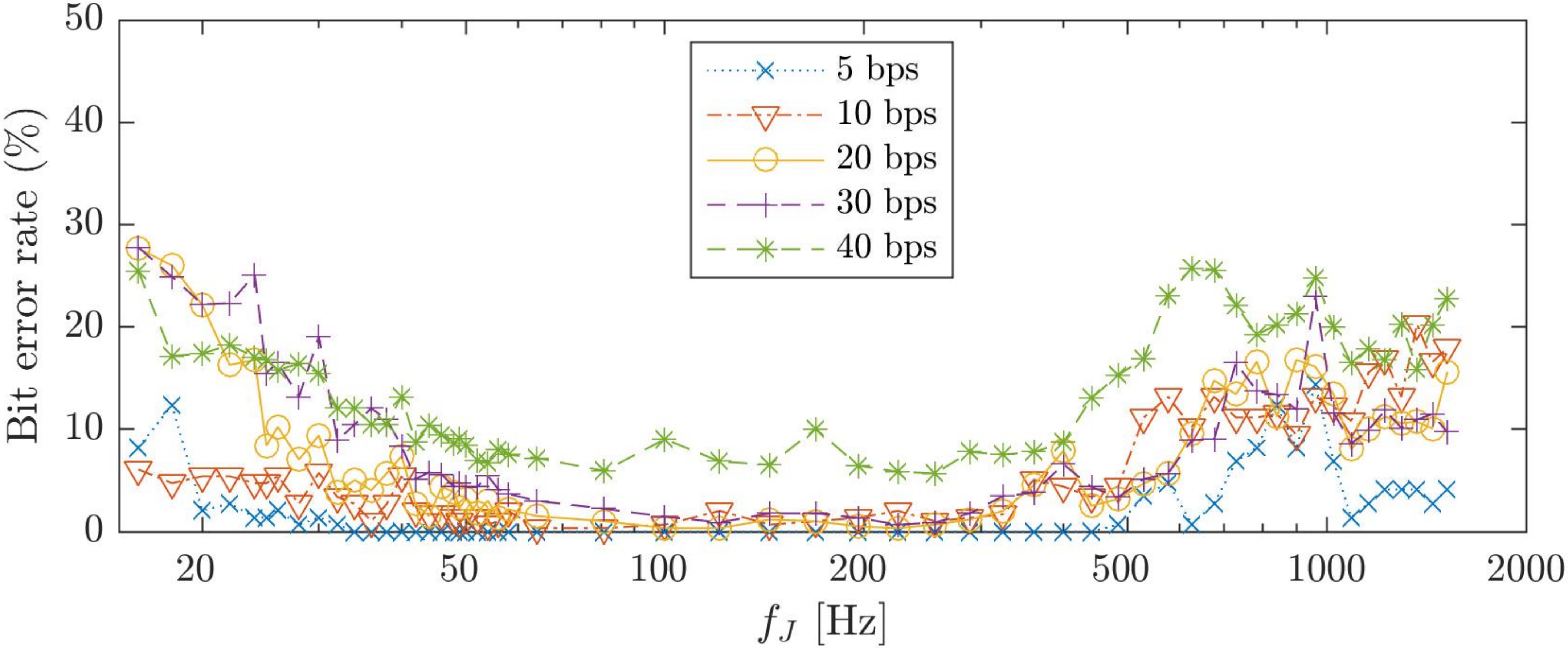
Keysight 33622A waveform generator

Tektronix RSA604 real-time signal analyzer

Results


Solid blue: Delay [sec]
Dotted red: trans. bits
0.04
0.02
0
1
2
3
4
5
6
Time [sec]

Results



5 bps
10 bps
20 bps
30 bps
40 bps
Bit error rate (%)
0
10
20
30
40
50
20
50
100
200
500
1000
2000
f_J [Hz]

Results

Successful data transfer at rates of 40 bits-per-second with <10% error rate.

Effective to a range of 15+ meters, works through walls.

Found functional at low transmission powers of -17 dBm, or 20 microwatts.

Micro-Jamming Done Passively

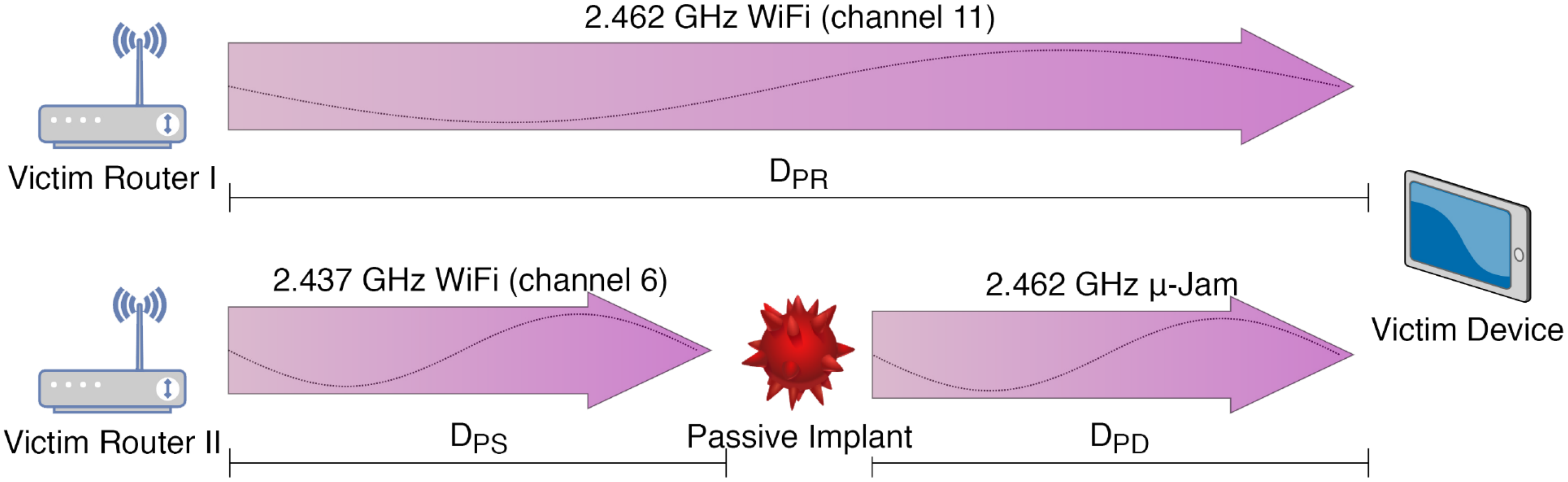
When an antenna switches its impendence in a given frequency, it modulates reflects any ambient radio signals while imposing a frequency shift.

Previous works[3] have used this phenomenon to shift one Wi-Fi channel to another while modulating data on top of it.

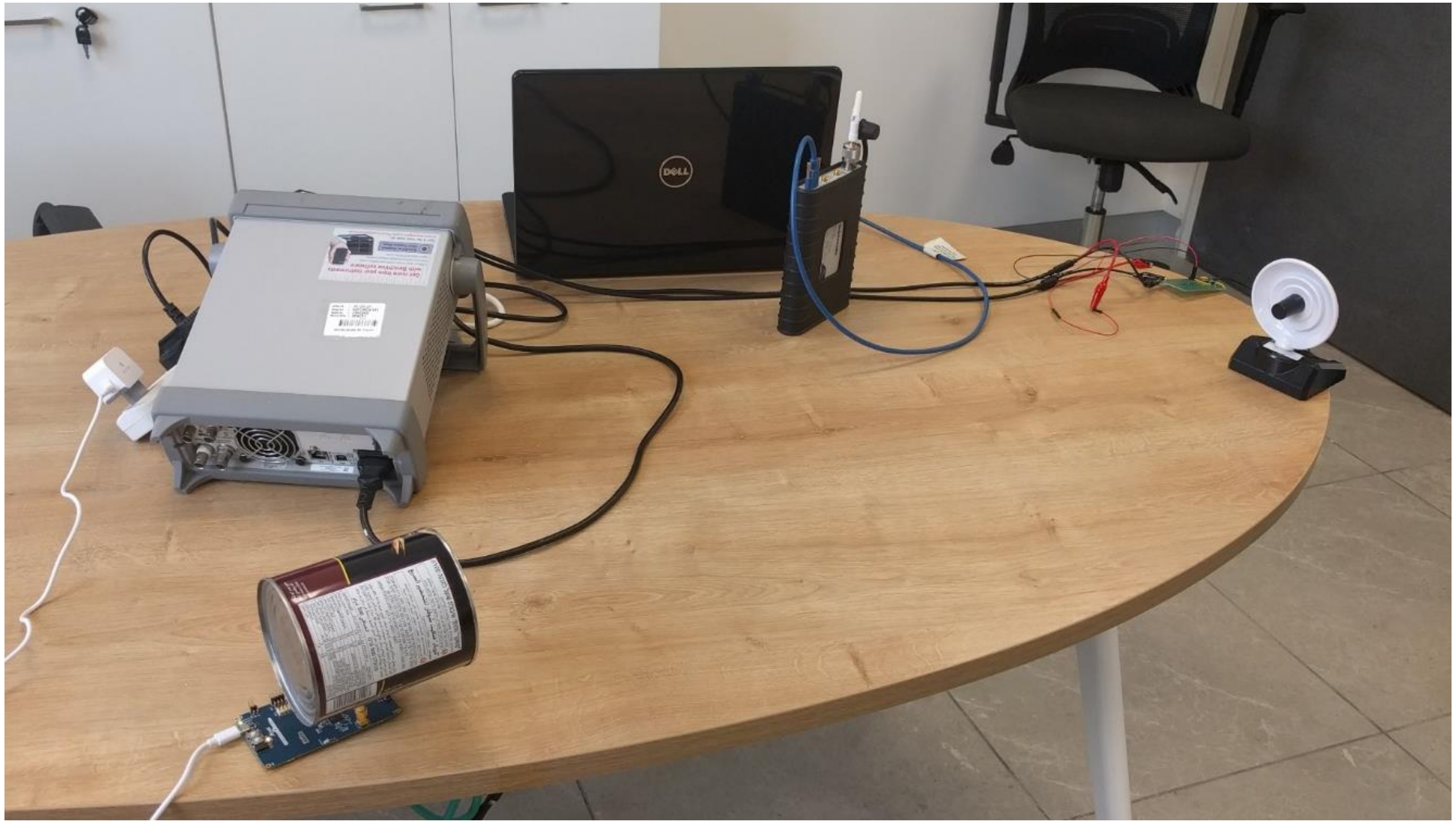
Using similar techniques, it is possible to jam a Wi-Fi channel using zero energy for transmission.

[3] Bryce Kellogg, Vamsi Talla, Shyamnath Gollakota, and Joshua R. Smith. Passive wi-fi: Bringing low power to wi-fi transmissions. 13th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2016, Santa Clara, CA, USA.

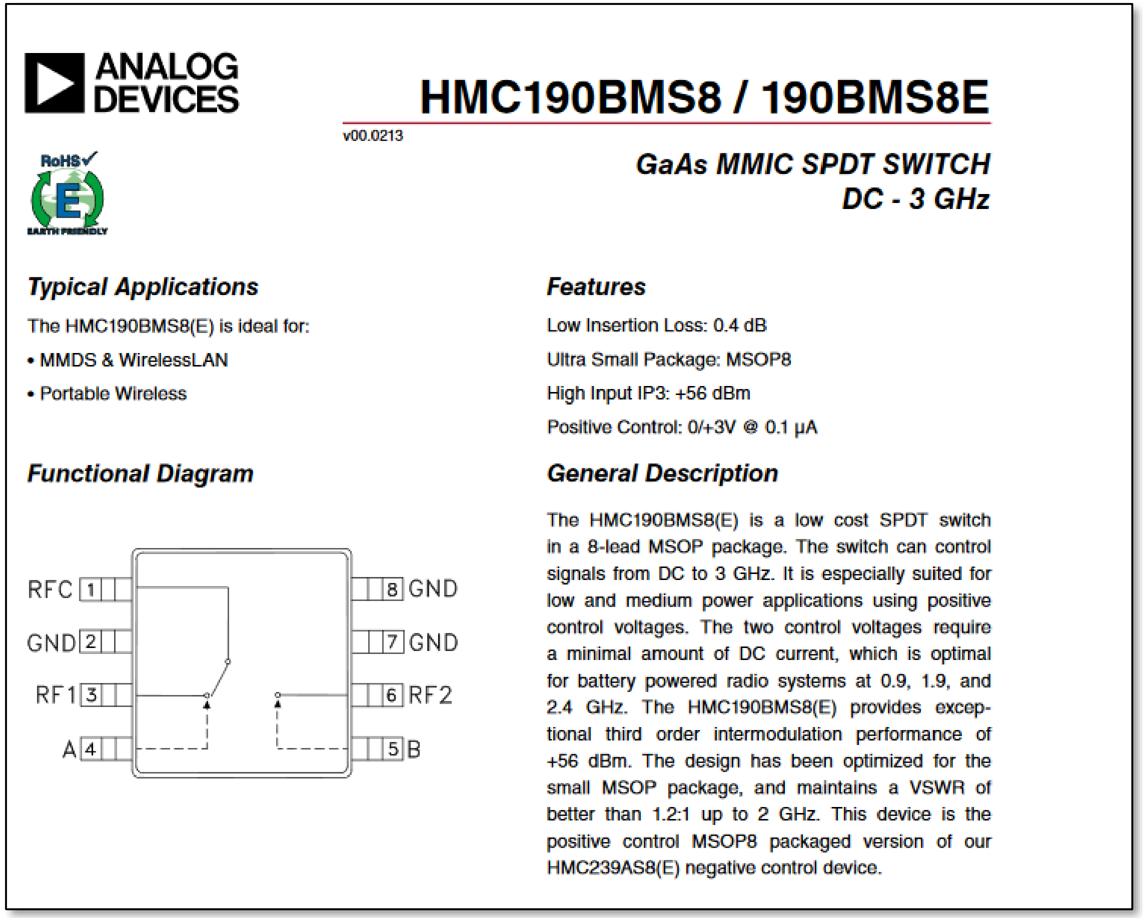
Test Setup - Passive



Test Setup – Passive



Test Setup – Passive



ANALOG DEVICES

HMC190BMS8 / 190BMS8E

v00.0213

RoHS✓ EARTH FRIENDLY

GaAs MMIC SPDT SWITCH
DC - 3 GHz

Typical Applications

The HMC190BMS8(E) is ideal for:

- MMDS & WirelessLAN
- Portable Wireless

Features

Low Insertion Loss: 0.4 dB

Ultra Small Package: MSOP8

High Input IP3: +56 dBm

Positive Control: 0/+3V @ 0.1 μA

Functional Diagram

RFC 1
GND 2
RF1 3
A 4
8 GND
7 GND
6 RF2
5 B

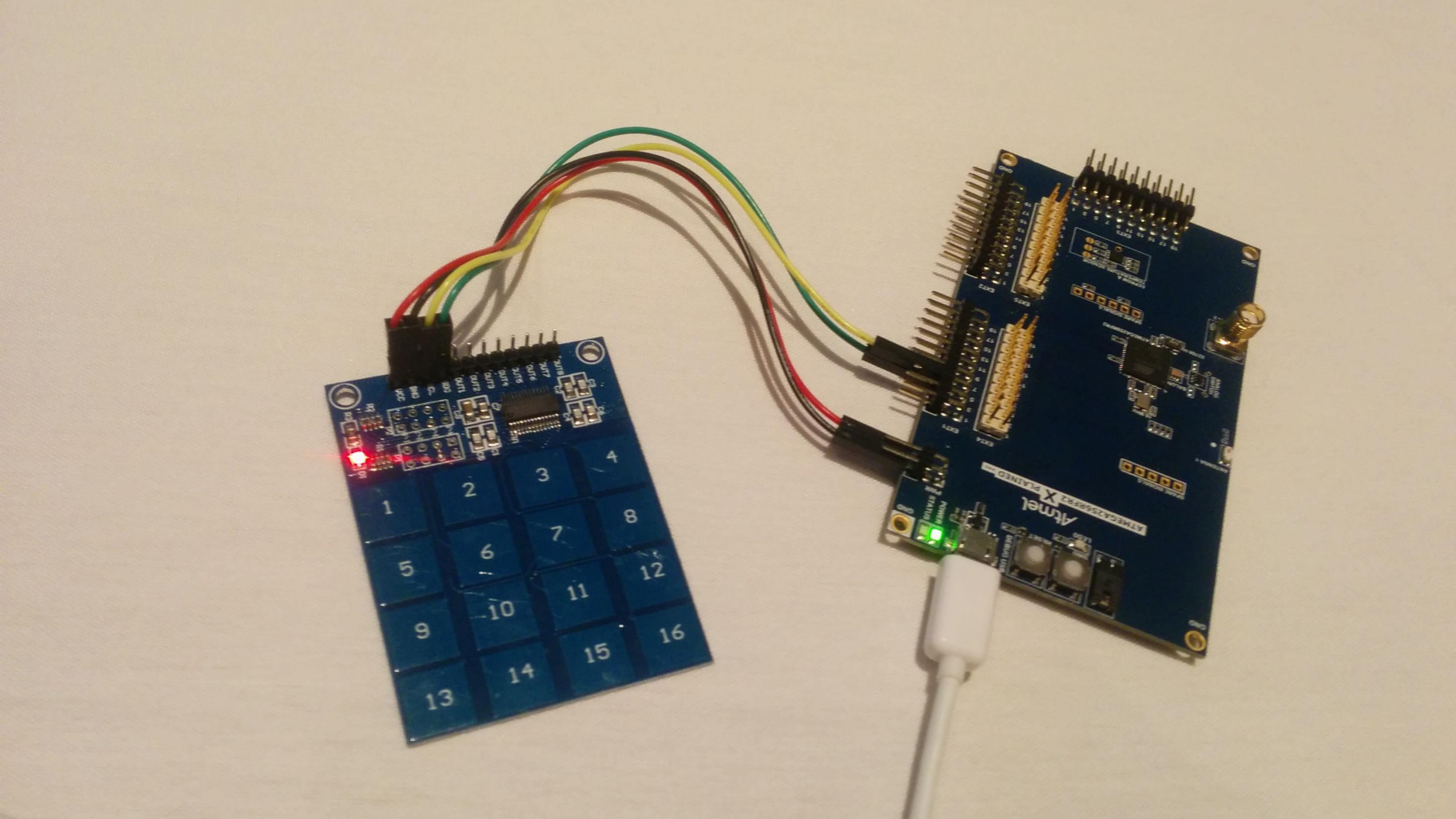
General Description

The HMC190BMS8(E) is a low cost SPDT switch in a 8-lead MSOP package. The switch can control signals from DC to 3 GHz. It is especially suited for low and medium power applications using positive control voltages. The two control voltages require a minimal amount of DC current, which is optimal for battery powered radio systems at 0.9, 1.9, and 2.4 GHz. The HMC190BMS8(E) provides exceptional third order intermodulation performance of +56 dBm. The design has been optimized for the small MSOP package, and maintains a VSWR of better than 1.2:1 up to 2 GHz. This device is the positive control MSOP8 packaged version of our HMC239AS8(E) negative control device.

Traditional Jamming vs Micro-Jamming (cont')

	Traditional Jamming	Micro-Jamming
Range vs transmission power	Small, must overcome existing signals	Large
Can be done passively?	Not effectively?	Demonstrated in the paper
Detectability	Shows in standard network logs	Hard to differentiate from noise

Demo


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
VCC
GND
SCL
SDO
OUT1
OUT2
OUT3
OUT4
OUT5
OUT6
OUT7
OUT8
ATMEGA256RFR2 X PLAINED
Atmel
POWER
STATUS
EXT1
EXT2
EXT3
EXT4
RESET
GND

Conclusions

Micro-jamming was shown as an effective development over traditional jamming as a covert channel.

Using micro-jamming, an implant can transmit over longer distances and use less power than with traditional jamming.

In addition, micro-jamming allows for lower-profile exfiltration of data that is harder to detect without actively looking with the right equipment.

Thank You – Any Questions?

Rom Ogen (romog@post.bgu.ac.il)

Omer Shwartz (omershv@post.bgu.ac.il)

Kfir Zvi (zvikf@post.bgu.ac.il)

Yossi Oren (yos@bgu.ac.il)

Come see our live demo at the USENIX poster session!

https://iss.oy.ne.ro/Microjam