DolphinAttack (Theoretical)

Lingyun Cao, Weijing Li

Abstract

DolphinAttack means those attacks to mobiles caused by inaudible sounds(out of people's audible range). Without detection by users, we can hack into the phones covertly and play roles like communication, jamming even communicate with mobile assistants! In the project, we leverages the non-linear systems in mobiles, which handles inaudible sounds without noticification.

The Problem and Idea

Problem:

(i). how to transform attack sounds into the inaudible range(>20kHz);

(ii). how to play it in way enabling the target to receive;

Idea:

SW: matlab;

HW: amplifier, ultrasonic speaker , signal generator;

Algorithm(SW)

Low-pass Filter

A low-pass filter on the normal signal, with frequency as 8kHz to remove high frequency part;

(will not affect human speech)

=>allow a lower carrier frequency for modulation;

Upsampling

Usually, sampling rate will be 48kHz or 44.1kHz => fit for sound below 24kHz or 22.05kHz;

We need at least 28kHz => not enough;

=> Before modulation, it should apply upsampling;

Ultrasound Modulation

AM modulation:

Smodu = n1Supcos(2πfct);

(n1 is the normalized coefficient;)

(fc should be at least 28kHz)

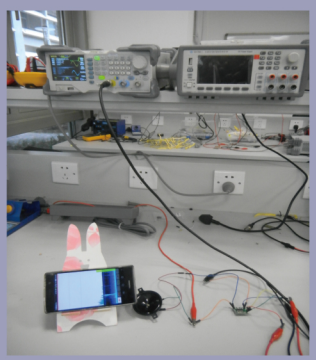
Carrier Wave Addition

Translate back to normal voice frequency range at the microphone for attacks;

(by non-linearity)

=> Sattack = n2(Smodu + cos(2πfct));

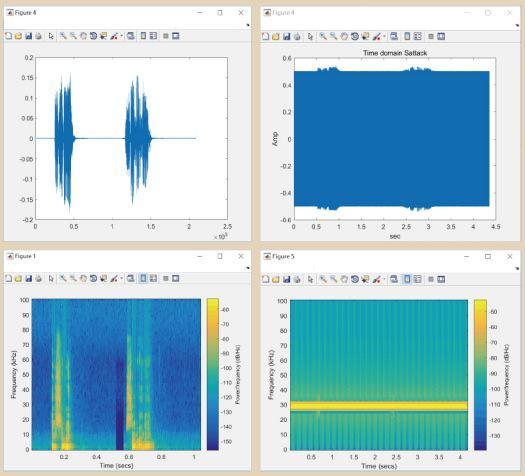
Hardware Design



Tested phone	HUAWEI P7 L09
Singnal generator	Rigol DG1000Z
(DAC)	Tektronix AFG 1006A
Speaker	5120 Ultrasonic speaker
Amplifier	PAM 8403

The above figure has shown the informatin of our testbed concluding the amplifier, speaker, phone(-source origin) and signal generator. During our experience, we found the Tek's and Rigol's signal generator is too poor to play the ultrasonic sounds(in .wav form), thus we turn into theoretical proof.

Implementation && Result

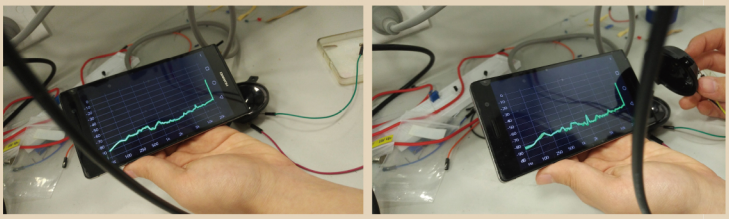


left-top: plot of original signal;

left-bottom:signal spectrum diagram of origin signal;

right-top: plot of attack signal;

right-bottom: signal spectrum diagram of attack signal;



These are photos showing our testing result of mobiles' non-linearity. Here two tones are set with frequency of 21kHz and 23kHz, resulting in a calculated outcome as 2kHz. It can see clearly that a new peak at 2kHz occured with little noise and the process keeps silent enough since humans can not hear sounds in either 21kHz or 23kHz.

Reference:

[1] Roy, Nirupam, H. Hassanieh, and R. Roy Choudhury. "BackDoor: Making Microphones Hear Inaudible Sounds." The, International Conference 2017:2–14.

[2] Zhang, Guoming, et al. "DolphinAttack: Inaudible Voice Commands." (2017).