**EarArray: Defending against DolphinAttack via Acoustic Attenuation**

**Rahavee Prabakaran**

The research paper addresses one of the most devasting attacks against voice assistants called “DolphinAttack”. In this attack attackers can modulate malicious voice commands onto ultrasounds and thus create inaudible voice commands. In this paper, a lightweight method called EarArray is discussed, that can not only detect such attacks but also identify the direction of attackers without requiring any extra hardware or hardware modification. The paper first starts by discussing the DolphinAttack, then presents the basics of attenuation of acoustic waves and gives the rationale why it can be used to detect such attack. Then popular smart devices are addressed and the feasibility of detecting DolphinAttacks is shown. The three stages of how inaudible voice commands are transformed are Ultrasound, Ultrasound & Sound and sound respectively. In stage 1, the voice commands are Amplitude-modulated on ultrasound carrier, in the second stage both ultrasound and the low-frequency voice commands are recovered by using the non-linearity of microphone hardware and in stage 3, high-frequency ultrasound component is filtered by the low-pass filter and only the voice commands remain. The paper considers three main sources for the acoustic attenuation namely the inverse-square law, sound absorption and diffraction. Using these three sources, the paper concludes that attenuation increases with acoustic frequency and distance. The paper then goes on to model the attenuation of audible and inaudible sound in the process of propagation. Then, the sound field distribution around a cylinder is simulated using COMSOL. By Theoretical Analysis, it is observed that the attenuation transfer function of attack signal is also related to the carrier frequency and the attenuation difference of different paths is more significant. Using Simulation results it is verified that the energy received by microphones in each channel are significantly different due to the attenuation and diffraction of sound wave when the frequency of incident wave is 25kHz, but it is uniform in the case of low-frequency source. The paper also analyses the results of verification of Acoustic Attenuation in which it is observed that the diffraction attenuation increases with acoustic frequency. Thus, the difference of high-frequency ultrasound received by the five microphones is higher than low-frequency sound. The design of EarArray system is described by three major components namely Audio signal preprocessing, Feature extraction and Attack detection & localization. In the workflow of EarArray, the audio signals are first captured from multiple microphones on a device and then fed into the detection component which includes pre-processing, feature extraction and attack detection. Later, the paper introduces the specifically-designed prototype of a microphone array and then the evaluation is elaborated. The experimental setup consists has a hardware setup where a benchtop transmitter, Bluetooth speaker are used, 25 volunteers were recruited to speak the 5 voices commands. The metrics to evaluate the performance are Accuracy, TNR, TPR and recall. The impact of distances, impact of angle, influence of carrier frequencies, impact of ambient noise, impact of different voice commands is also studied. The paper’s future work includes overcoming the problem that mobile phones cannot read multi-channel data at the same time, extracting field patterns from more different types of voice assistant devices.

**Three strong points:**

1.Paper clearly describes the Experimental setup to study the defense method.

2.Results and analysis have been picturized effectively.

3.The hardware setup is clearly understood through the image.

**Three weak points:**

1.There is not much description and study on DolphinAttack, before addressing the defense against it.

2.The defense mechanism is restricted on the concept of Acoustic Attenuation only.

3. No description of why Acoustic Attenuation is only used to devise a defense technique.