Let's make some music

UNLOCKING THE LIMITLESS POSSIBILITIES WITH ULTRASONICS FOR FRICTIONLESS DIGITAL BANKING

In 2022, the total amount of smartphone shipments reached 1.21 billion units worldwide. Each smartphone has a speaker and a microphone. Additionally, 130 million households are home to at least one smart speaker, which is expected to rise to 335 million in the next 5 years. While it is unrealistic to be online 24/7 with no drops in coverage or speed—especially while traveling—losing connection can be a significant problem for organizations.

Can sound solve the problem?

While Alexa, Siri, and others have been around for a while and require a human being to communicate with them using voice. Now, just imagine if all these devices are able to communicate with each other when in proximity, without the need for office/network/wi-fi, and in a manner that is inaudible to the human ear.

Google's Nearby Messages API or Starbucks location beacons are high-frequency data-over-sound applications that are popular with developers and users. However, these high-frequency beacons are not suited to delivering text and sensitive data because they are prone to interference from ambient sounds and heavily depend on the performance of the Digital-to-Analog converter (DAC) and the Analog-to-Digital converters (ADC).

Data-over-Sound (DoS), also known as Aerial Acoustic Communication (AAC) is a communication protocol that utilizes signals at the upper bounds of human hearing (above 15 kHz).

DoS can convert any existing speaker into a data transmitter and any device with a microphone into a data receiver. The basic idea of data-over-sound is no more complex than a traditional telephone modem. Data is encoded into an acoustic signal, which is then played through a medium (typically the air, although it could equally be a wired telephone line or VoIP stream) and received and demodulated by a 'listening' device.

This wireless communication protocol has advantages over the widely used Bluetooth and Wi-Fi for localized data exchanges within a small physical distance. It has advantages in terms of secure and localized data exchanges when compared to radio waves, given that the acoustic waves (periodic pressure disturbances) with wavelengths near the ultrasonic range do not pass-through barriers and are simply reflected off the walls of a typical room.

The only hardware DoS requires is a speaker and a microphone, which are present in audio-video equipment and every smartphone; and increasingly, in wearables, smart appliances, and IoT devices.

Data-over-Sound versus other methods

DoS opens a wide array of use cases across industries and has the potential to redefine user experience through seamless and frictionless user journeys. It is steadily gaining popularity in several industrial and consumer applications such as entry systems for public transport, contact-less payments, inventory management, and proximity-based customer engagement — all using sound waves.

Example: Sound-based authentication for banking

One of the many possible use cases is that of password-less authentication. Presently, two-factor authentication

The Following key features cover the most used protocols:

	DoS	QR	NFC	Bluetooth	Wi-Fi
Two-Way Communication	Yes	No	No	Yes	Yes
One-to-Many Broadcasts	Yes	No	No	No	No
Non-Line-of-Sight Transmissions	Yes	No	No	Yes	Yes
Broadcasts Confined to Room Boundaries	Yes	Yes	Yes	No	No
Typical Max Range	100m		20cm	100m	50m

mechanisms require the user to interact with the phone too- for example, to copy a verification code received through an SMS or an authenticator app to the browser, resulting in multiple steps and causing friction.

Let us look at the modern way of authentication. Password-less authentication is a method of verifying a user's identity without requiring them to enter a password. Instead, password-less authentication relies on other factors such as biometric authentication or a one-time code to verify the user's identity. Here are the steps involved in the password-less authentication process:

- The user initiates the login: Process on the mobile banking application or website.
- Identity verification request: The mobile banking application or website sends a request to the user's device to verify their identity using a biometric authentication method, such as facial recognition, fingerprint scanning, or voice recognition.
- Biometric verification: Confirms identity for verification.
- Token generation: If the user's identity is verified successfully, the mobile banking application or website generates a token that is sent to the user's device.
- Token validation: The user's device sends the token back to the mobile banking application or website, which validates the token to confirm that it was generated by the correct user and device.
- Access granted: Once the token is validated, the user is granted access to their account.

Password-less authentication is becoming increasingly popular as it is considered more secure than traditional password-based authentication methods. It eliminates the risk of stolen or compromised passwords and reduces the need for users to remember complex passwords.

Here are the user journey steps for ultrasonic sound-based password-less authentication in a mobile banking application:

- The user initiates login: The user opens the mobile banking application and initiates the login process.
- Authentication request: The mobile banking application sends a request to the sound-based authentication server to verify the user's identity using unique sound patterns.
- Access granted: If the user's sound pattern is authenticated successfully, the server sends a response to the mobile banking application indicating that the user is authenticated, and access is granted to their mobile banking account.

TCS BaNCS The Research Journal
https://joom.ag/QmNd

Compared to the current ways of password-less authentication, no user action is required in the form of picking up the phone, typing in the OTP/Passkey, etc. Using DoS, the second authentication factor is the proximity of the user's phone to the device being used to log in. It uses ultrasonic sound waves to transmit encrypted digital data between two devices with a speaker and a microphone. Being ultrasonic and with the speaker's capability to recognize different frequencies, the perceived issues of being in a noisy area during the process are also minimal. Most importantly, this does not require interaction between the user and his phone. It also solves the problem of working with no/low network connectivity.

Is this Safe?

Is it possible to hack the data transferred through sound? DoS appears to be more secure than SMS OTP or Authenticator-based ones and makes up for the shortcomings of Bluetooth/NFC/QR-based methods.

Data-over-sound (DoS) is a technology that uses sound waves to transmit data. Here are some ways to secure data-over-sound transmissions:

- Use strong encryption: Encrypting the data before it is transmitted using sound-based communication is essential. Strong encryption ensures that the data cannot be read or decoded even if the transmission is intercepted.
- Verify the sender and receiver: The sender and receiver of data-over-sound transmissions should be verified to ensure that they are authorized. Sound-based communication systems can use sound signatures, like voice biometrics, to verify the sender and receiver's identities.
- Implement anti-jamming technology: DoS transmissions can be susceptible to interference or jamming from other sources. Anti-jamming technology can be used to protect against such interference and ensure reliable transmission.
- Use frequency hopping: Frequency hopping can be used to spread the signal across multiple frequencies, making it harder for attackers to intercept or interfere with the transmission.
- Limit the transmission range: Limiting the transmission range of the sound-based communication system can help prevent unauthorized access to the transmitted data.
- Regularly update the system: As with any security system, keeping the data-over-sound system up to date with the latest security patches and updates is crucial. Regularly testing and updating the system can help protect against new threats.
- By following these best practices, you can secure data-over-sound transmissions and ensure that your sensitive data is protected from unauthorized access.

DoS is one of the many ways to eliminate friction and by far the best use case for frictionless journeys right at the start.

Conclusion

By harnessing the power of sound, Data-over-Sound has emerged as a reliable and cost-effective way to exchange data between devices within a small physical distance. With the increasing number of smart speakers and connected devices in homes. Businesses, and public spaces, DoS is providing a host of opportunities for firms to increase their efficiencies, improve user experience and drive customer engagement.

DoS opens a wide array of use cases across industries and has the potential to redefine user experience through seamless and frictionless user journeys.

Subrato Bhattacharya
Senior Consultant,
TCS Financial Solutions (TCS BaNCS)