Sending and Receiving Data using Audio

- with Time-based Keying Technique

Detailed Proposal

PRIMARY SUPERVISOR
Tom Carroll

SECONDARY SUPERVISOR
Sebastian Coope

STUDENT
Shuoyang Zheng (Jasper)
201377421
sgszhen8

1. Project Description

Along with Wi-Fi, Bluetooth, Near-field Communication (NFC), the future of connectivity will be a combination of technologies working together to achieve the ubiquitous, frictionless connectivity, especially in the Internet of Things (IoT). In this context, engineers have been continuously exploring new possibilities of data transmissions. One solution rising to address these inevitable demands for better connectivity is data-over-sound. It enables devices to send and receive data by produce or recognise audible or inaudible sounds. With clear and practical affordances of data-over-sound, including its seamless integration, ability to work offline, scalability, it was already implemented in a few innovative systems.

However, significant concerns in data-over-sound are related to security. Since it is a broadcasting-based technique, and the transmitted signal is audibly exposed in the environment, it could be easily recorded and reproduced maliciously to disrupt the system (also known as replay attacks).

In this project, I hope to design and implement a data transmission system with the data-over-sound technique that is resistance to replay attacks. The project will look into digital signal processing (DSP), including data modulation and demodulation, then investigate in time-based keying technique to confront replay attack. It will also evaluate the implemented system statistically.

2. Aims & Objectives

The project aims to develop a device-to-device communication system based on data over sound technique. The system will consist of a sender device and a receiver device, allow users to receive text broadcasted from an authorised sender.

2.1 Objectives

1. Design a communication protocol between the sender and the receiver.
2. Design an authentication mechanism between the sender and the receiver.
3. Implement a sender that reads the text input by the user and translate it to audible sound signals.
4. Implement a receiver that:
   1. recognises sound signal produced by authorised sender devices.
   2. translates the sound signal to original texts and display them to the user.
5. Both the sender and the receiver should be implemented on the accessible platform.
6. Carry out a testing plan to:
   1. ensure the communication system works properly.
   2. ensure the receiver could perform authentication check to only react to authorised senders.
   3. evaluate the transmission accuracy of the system.
   4. evaluate the transmission rate of the system.
   5. evaluate the maximum amount of ambient noise that the system could confront.
   6. evaluate the performance of the system under different situations (variables include the distance between sender and receiver, the volume of the sender).

3. Key Literature & Background Reading

During the background reading period, various sources from the following three aspects were collected to support the project.

1. The background and the context of data over sound technology
2. Related works on data over sound and their challenges
3. Technical materials that are related to the project

3.1 Background and Context

The background of data over sound technology was reviewed to ensure that the topic of this project would meet a real need in the context of the Internet of Thing (IoT).

The growing demand for better connectivity on the IoT has raised the expectations for even the most basic smart devices to securely stay connected to other home appliances or mobile devices [1]. Along with Wi-Fi and Bluetooth, engineers have been continuously investigating new possibilities of data transmissions. In this context, data-over-sound technology has real potential to provide frictionless connections.

Comparing to traditional alternatives such as Bluetooth and Wi-Fi, data over sound provide the following advantages:

1. It provides seamless integration without the need for prior setup or configuration [2].
2. It works in offline environments that have no network access [3].
3. It is scalable, allows one-to-many or many-to-one settings [2].
4. It is compatible with machines and devices of different platforms as long as the device could process and produce audio [3].

3.2 Related Works and Challenges

Several existed works have shown that data over sound technique could be applied to varieties of context.

Works such as SonicData have utilised data over sound technique to broadcast information in public space [5], the implementation includes responding to traffic updates, receiving charity advertisement, notifying a final boarding call. Similarly, the work of ChirpCast presents a system for broadcasting network access keys to laptops by sound [6]. These projects have successfully developed robust and flexible data transmitting systems. Meanwhile, companies such as Sonarax have presented live demos utilising data over sound technique to perform two-factor authentication to log in to a website [7].

A few works also suggested different options for data over sound. The demo presented by Quiet Modem Project allows users to transmit data with inaudible ultrasonic sound [8]. Although the bitrate was lower than using audible sound frequencies, it gives an option for sending data through a channel where users would prefer not to hear the sound signal.

However, considerable challenges in data-over-sound were highlighted by previous researchers. Concerns include the reverberation (i.e. echo), the Doppler Effect, and power efficiency [4]. Also, security is the primary issue when it comes to data over sound. Although as in all communication protocols, data encryption method such as RSA, AES could be applied during the communication process, it is still easy to face the risk of replay attacks. In this situation, the attacker might broadcast pre-recorded sound to disrupt the communication system.

Therefore, to confront the primary concerns, replay attack, one of the objectives of this project will be to design and implement an authentication mechanism in the data over sound communication system.

3.3 Technical Sources: Modulation Schemes

According to previous research, there is not yet any standard protocol for encoding or decoding in data over sound [4], even though researchers have already conducted varieties of attempts. A general setting would be a modulator block consists of two oscillators with an input binary sequence and a clock [9], each producing signals according to a modulation scheme. Two possible modulation schemes are listed below.

Frequency Shift Keying

Frequency Shift Keying (FSK) transmits data by shifting the frequency of the channel carrier. [10]

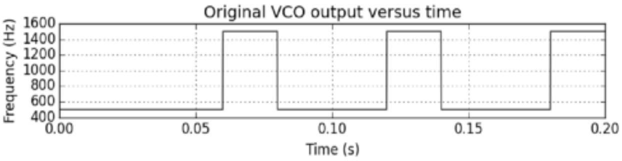


Figure 1: Frequency Shift Keying

Phase Shift Keying

Frequency Shift Keying (FSK) transmits data by shifting the phase of the channel carrier [10].

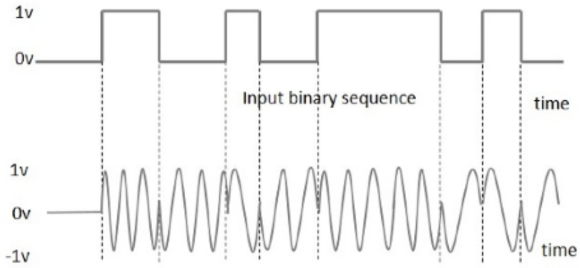


Figure 1: Frequency Shift Keying

According to the experiment conducted by the ChirpCast team, real-time data communication could be performed at a maximum bitrate of 4bps using Frequency Shift Keying, and at a maximum bitrate of 200bps using Differential Phase-shift Keying. In the development stage, both modulation schemes could be taken into consideration.

3.4 Technical Sources: Data Encryption

Time-based One-time Passwords (TOTP) could be used as the encryption method to prevent replay attacks. However, this method requires a clock that is roughly synchronised to the sender and the receiver device [11].

4. Development Process & Method

The project methodology will follow iterative development.

Stage 1: Implement a system that could perform Frequency Shift Keying, but not data encoded.

- A sender that is able to produce modulated binary data into audio
- A receiver that is able to demodulate and recognise the audio as binary data.

Stage 2: Design and Implement the communication protocol to the system.

- Implement a sender that is able to convert text messages to binary data that is ready to be modulated.
- Implement a receiver that is able to convert the recognised the demodulated binary data as text messages.

Stage 3 (Evaluation I): Evaluate the reliability and the performance of the system according to the testing plan.

Stage 4: Implement the time-based keying technique to the system.

- Implement a sender that is able to encrypt the text message with a time-based key.
- Implement a receiver that is able to authorise the received signal.

Stage 5 (Evaluation II): Evaluate the reliability and the performance of the system according to the testing plan, compare the result with Evaluation I).

Stage 1 will be implemented in Python 3.7, Stage 2 and Stage 4 will be first implemented in Python 3.7, and then transfer to the iOS platform via Pyramid. After each stage, the code and documents will be back up to GitHub.

5. Data Sources

There will be no external dataset used in the project. Text message used in the testing process will be self-generated pain text.

6. Testing & Evaluation

The development is driven by statistical testings to estimate the reliability and the performance of the system. The testing plan aims to evaluate the system according to the following criteria:

- Data transmission accuracy
- Authentication accuracy
- Data transmission rate
- Noise Immunity (The amount of ambient noise that the system could confront, as well as the ability to recover from a corrupted noise event)
- The minimum loudness of the system.

The test will also investigate in the relation between the five criteria (e.g. a lower loudness might introduce a lower accuracy, etc.)

7. Ethical Considerations

The project will be conducted in accordance with COMP390 Ethical Guideline.

A few existed works were reviewed in the design stage, and this project will retain its originality.

In the development process, open-source libraries related to audio synthesise, audio analysis will be used moderately, reference will be included in the system and the documentation.

In the testing process, original analyses and experimentations will be performed; all the data shown in the project will be genuine; there will be no covert research in the testing process.

8. BCS Project Criteria

Practical and Analytical Skills / Solution Evaluation

The project aims to investigate the development of data-over-sound, analyse the challenges in the technology, then propose a solution and examine that solution. There will be a full implementation of the design to realise the solution practically. The performance of the system will be evaluated twice (discussed in Chapter 4 and Chapter 6), to examine the solution critically by experimentations.

Innovation

While the secondary information has shown that the challenges include the concern on replay attack (discussed in Chapter 3.2), the project confronts the security implications of data-over-sound, innovatively test the possibilities of applying a time-based keying technique between the modulation and demodulation process.

Needs and Contexts

If the results show that the designs and the implementations are acceptable, this project will provide a preliminary alternative to the prevention of replay attack in data-over-sound. As transmitting data over the sound is being seen as a future-proof technique in the Internet of Things, later developments of this solution could maintain a secure data transmission between smart home appliances. And it will pave the way for the countermeasures of replay attacks.

Self-management / Self-evaluation

The project covers the topics related to digital signal processing (DSP), modulation and time-based keying. However, it will be managed by compact project plans and documentation recordings. Also, the process of the project will be evaluated at the end of the project.

9. Software & Hardware Resources

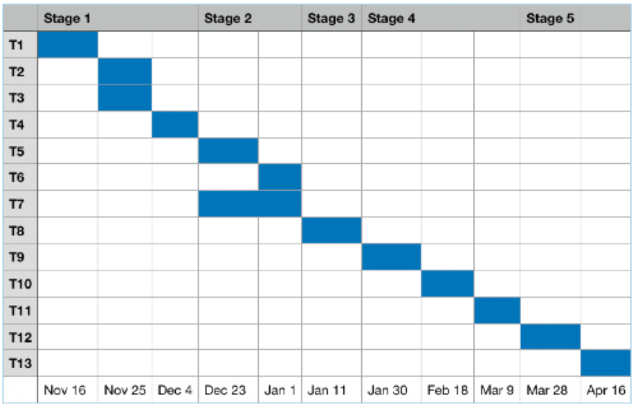
Device Usage	
Personal laptop (Macbook Pro 15 2019)	Design / Coding / Document Records
External Hard Drives	Backups
iPhone X running iOS 14.3 Testing	Testing

Software Usage	
Spyder 4.1.4	Development (Python)
Xcode 12	Development (Swift)

There will be no external services used in the project.

10. Project Plan

Task 1	Set up the environment and libraries
Task 2	FSK modulation, T1
Task 3	FSK demodulation, T1
Task 4	Implement the Stage 1 design
Task 5	Text messages to binary data
Task 6	Design the protocol
Task 7	Interface design
Task 8	Implement Stage 2 design
Task 9	Evaluation I
Task 10	Time-based keying
Task 11	Implement Stage 3 design
Task 12	Evaluation II
Task 13	Demo preparation



11. Risks & Contingency Plans

Risk	Contingency	Likelihood	Impact
Having problems implementing the system in iOS	Change the system to a web document.	Medium	An ideal prototype could not be achieved.
Running out of time	Cancel the implementation on iOS, only implement the system in Python shell	Low	An ideal prototype could not be achieved, would affect the quality of the demonstration.
Lost, reset or broken of the laptop.	Transfer the workflow to the lab computer, or my spare windows laptop.	Low	Cost extra time

12. References

1. IEEE Innovation, "*Transferring Data Over Sound"* [Online]. Available: https://innovationatwork.ieee.org/transferring-data-over-sound/ [Accessed: 10th Nov 2020]

2. Electronic Design, "*Sending Data Over Sound: How and Why?*" [Online]. Available: https://innovationatwork.ieee.org/transferring-data-over-sound/ [Accessed: 10th Nov 2020]

3. Forbes, "*How Data-Over-Sound Will Ensure A Permanently Connected IoT World"* [Online]. Available: https://www.forbes.com/sites/simonchandler/2019/10/18/how-data-over-sound-will-ensure-a-permanently-connected-iot-world/ [Accessed: 10th Nov 2020]

4. SONARAX, "*Why it's so challenging to develop data over sound technology?*" [Online]. Available: https://www.sonarax.com/post/why-its-so-challenging-to-develop-data-over-sound-technology-why-the-other-protocols-failed [Accessed: 10th Nov 2020]

5. A. Nittala. X. Yang, et al, "*SonicData: Broadcasting Data via Sound for Smartphones*" in PRISM: University of Calgary's Digital Repository, October 2014. [Online]. Available: https://www.researchgate.net/publication/275337145_SonicData_Broadcasting_Data_via_Sound_for_Smartphones [Accessed: 10th Nov 2020]

6. F. Iannacci. Y. Huang, "*ChirpCast: Data Transmission via Audio*" Networking and Internet Architecture, August 2015. [Online]. Available: https://arxiv.org/abs/1508.07099 [Accessed: 10th Nov 2020]

7. SONARAX, "*Sonarax Free Demo Application?*" [Online]. Available: https://www.sonarax.com/demo-the-sonarax-technology-using-our-demo-app [Accessed: 10th Nov 2020]

8. brian-armstrong, "*Quiet Modem Project*" [Online]. Available:https://github.com/quiet/quiet/ [Accessed: 10th Nov 2020]

9. Tutorialspoint, "*Frequency Shift Keying*" [Online]. Available: https://www.tutorialspoint.com/digital_communication/digital_communication_frequency_shift_keying.htm [Accessed: 10th Nov 2020]

10. Tutorialspoint, "*Phase Shift Keying*" [Online]. Available: https://www.tutorialspoint.com/digital_communication/digital_communication_phase_shift_keying.htm [Accessed: 10th Nov 2020]

11. J. Todd, "*Sending encrypted data with sound*", SD Times [Online]. Available: https://sdtimes.com/data/sending-encrypted-data-with-sound/ [Accessed: 10th Nov 2020]