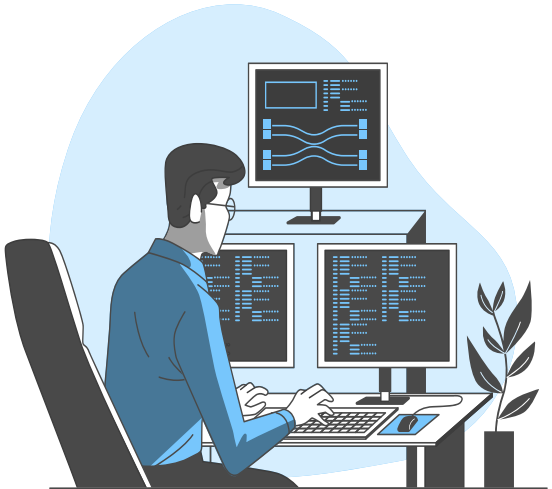
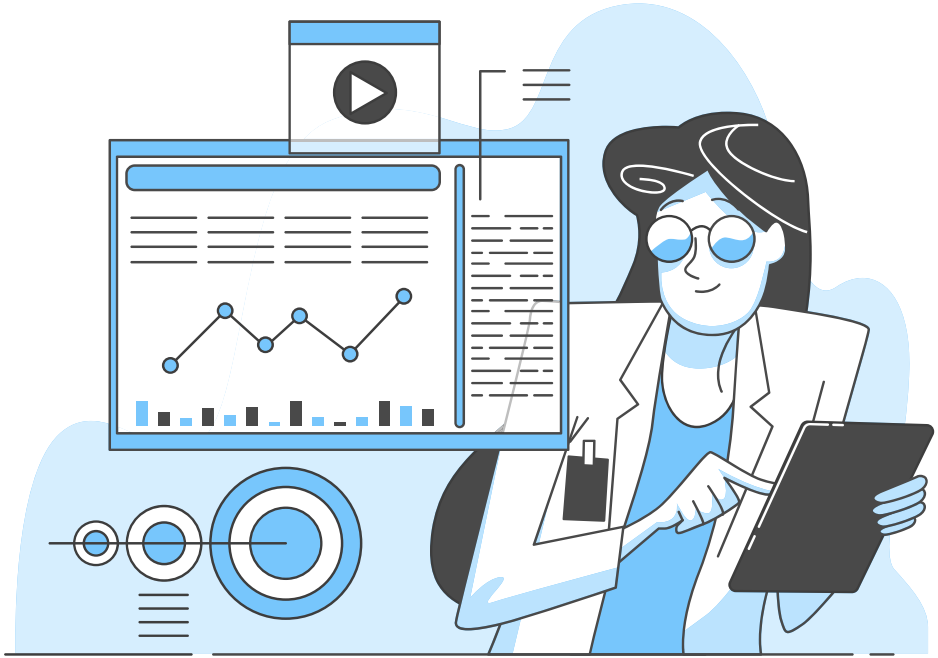
Exploiting Privacy Leakage of User Location From Smartphone IMU



Group number: Z2
Student 1: POON, Wai Hong, 1155125126
Student 2: MA, Yi Tsung, 1155125509
Supervisor: Prof. YAN, Zhenyu

Table of Contents



01

Introduction

Why this project?

Accuracy

Higher accuracy for contact tracing

Inconvenience of QR code

QR code scanning requires a longer time.

Security

A safer mean to prevent information leakage.

“LeaveHomeSafe”

Not user-friendly for elderly

Difficult to scan with poor quality camera

Block the entries with many people trying to scan

Redundant usage. Need to scan back the vaccine records.

02

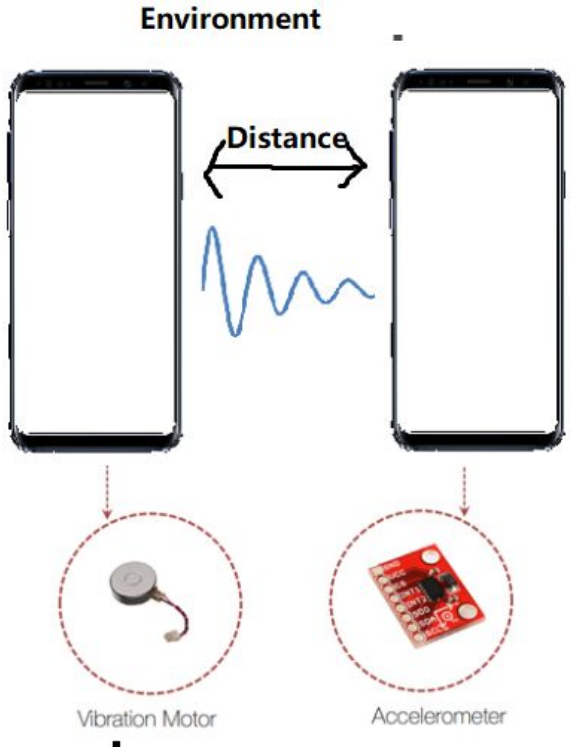
Methodology

2.1 Modulation and Demodulation
2.2 Comparison between ASK and FSK
2.3 Mobile Application
2.4 App Design
2.5 Morse Code
2.6 Encode and Decode

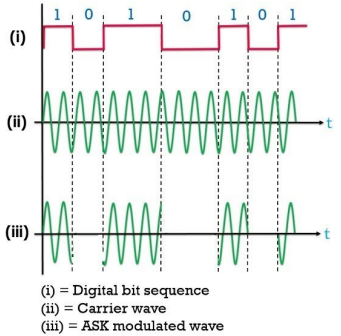
2 Methodology
Our Setup

Keys:

1. Environment noise
2. Distance between devices
3. Message transition



2 Methodology
2.1 De/Modulation: Amplitude Shift Keying (ASK)

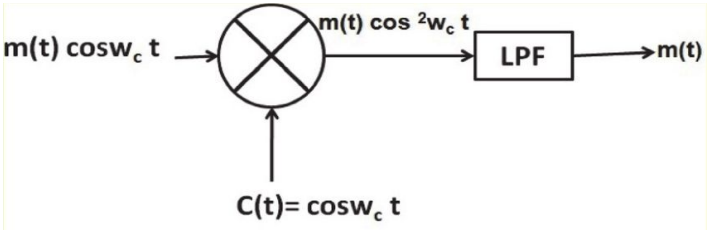


(i) = Digital bit sequence
(ii) = Carrier wave
(iii) = ASK modulated wave

ASK is utilized to modulate the digital signal

Bit values are assigned to discrete amplitude levels .

. . .



2 Methodology
2.2 Comparison between ASK and FSK

Why ASK but not FSK (Frequency Shift Keying)?

FSK assigns bit values to discrete frequency levels which requires manipulation of frequency.

The **linear vibration motors** used by most of the smartphones nowadays **do not** support frequency manipulation.

...

2 Methodology
2.3 Mobile application

An application that controls the vibration patterns of the smartphones

(1) Create non-repeatable vibrations
(2) Create repeatable vibrations
(3) Create custom vibration patterns
(4) Control the strength (Amplitude) of the vibrations

...

```
@RequiresApi(api = Build.VERSION_CODES.O)
private void createWaveFormVibrationUsingVibrationEffectAndAmplitude() {

    long[] mVibratePattern = new long[]{1000, 1000, 2000, 2000, 2000, 1000};
    int[] mAmplitudes = new int[]{0, 255, 0, 255, 0, 255};
    // -1 : Play exactly once

    if (vibrator.hasAmplitudeControl()) {
        VibrationEffect effect = VibrationEffect.createWaveform(mVibratePattern, mAmplitudes,  repeat: 0);
        vibrator.vibrate(effect);
    }
```

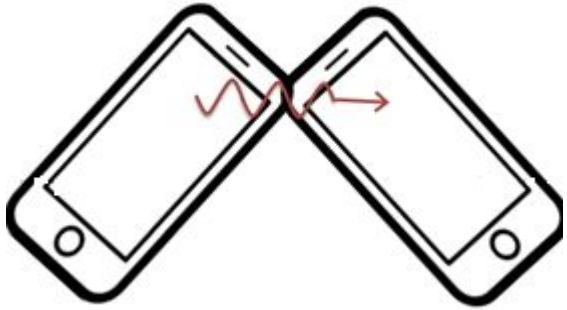
2 Methodology
2.4.1 App Design

Sender: transform message in vibration and transmit with vibrator
Receiver: sense data from the change in accelerometer

Key points:

1. Vibrator
2. Accelerometer
3. Signals sensing/extraction
4. Encoding and decoding

...

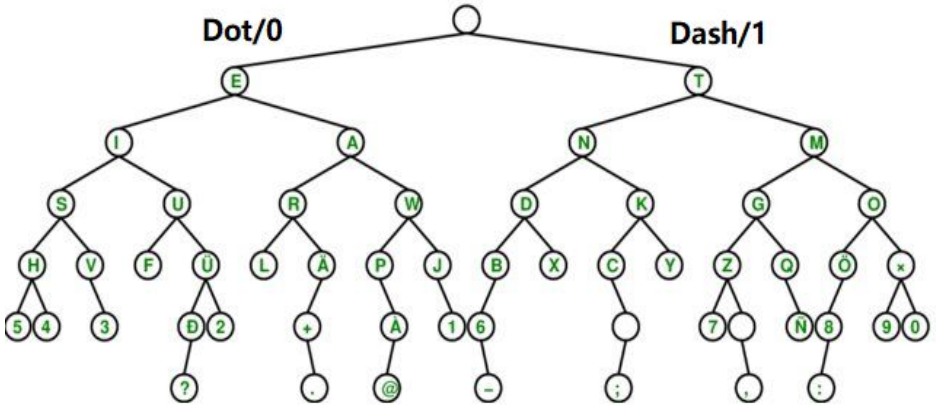


2 Methodology
2.5 Morse Code

Converts Morse code into vibration patterns.

Element	Time
Dot (●)	1 time unit
Dash (▬)	3 time units
Inter-element gap	1 time unit
Short gap between letters	3 time units
Medium gap between words	7 time units

...



2 Methodology
2.5.2 1 and 0 Morse Code

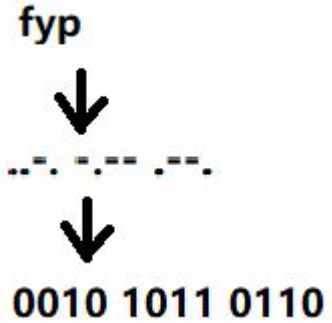
Make it more accessible and easier to communicate because the 3 time units of dash become 1 time unit.0 -> no vibration; 1-> 1 time unit vibration

For example the morse of “fyp” require 6 dots and 6 dashes which equal to 6 x 1 + 6 x 3 = **24 time units**

But the 1 and 0 morse only require **12 time units**

Half of the time is saved

...



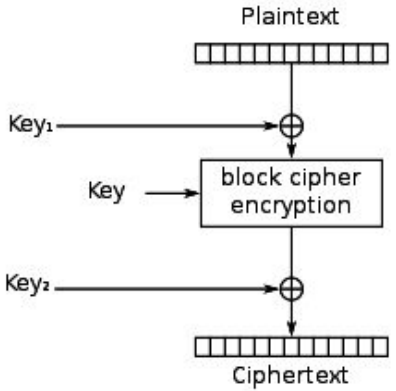
2 Methodology
2.6.1 Encode and Decode

Gap filler

we use the symbol ä to fill the gap between letter which represent as 1010.

XOR method

After filling the gap between the binary morse code. We use XOR logic to encrypt the binary with random key given from server.



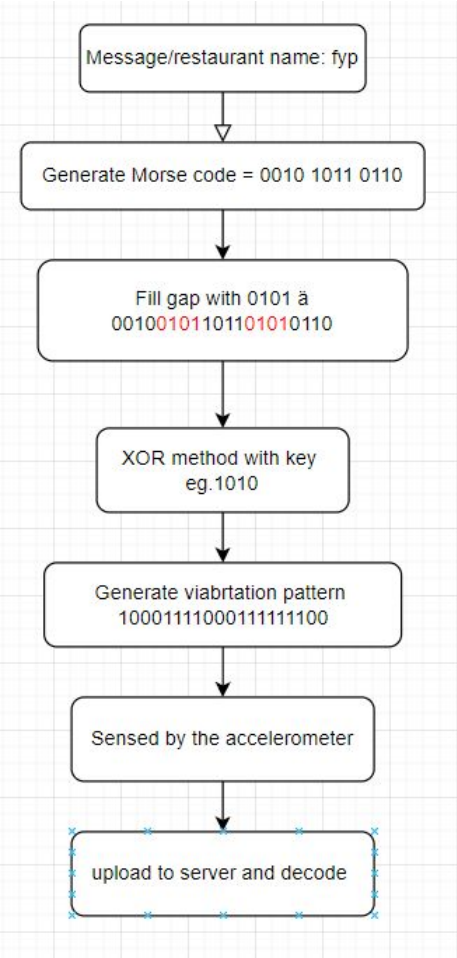
...

2 Methodology
2.6.2 Encode and Decode

The message will be:

1. Changed to Morse Binary format
2. Encrypt by XOR method
3. Send to other device as vibration
4. Received by accelerometer
5. Upload to server with also the user's info
6. Server decoded the message.

...



03

Testing and result

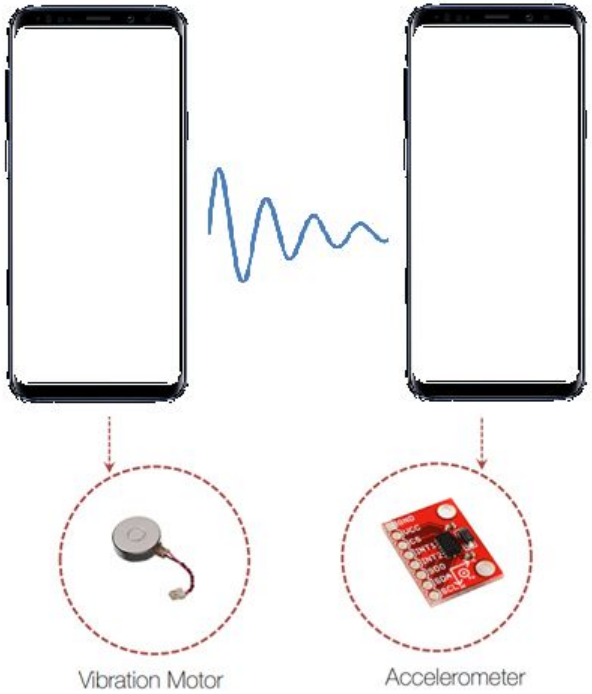
3.1 Mobile Application
3.2 Matlab Simulation

3 Testing and result
3.1 Testing variables

Tested by one sender phone and one receiver phone on:

1. Same accelerometer sampling rate 500 Hz
2. Different acceleration speed From 0.5f to 1.75f
3. Different medium. Glass, wood table, ceramic tile.
4. Different distance.

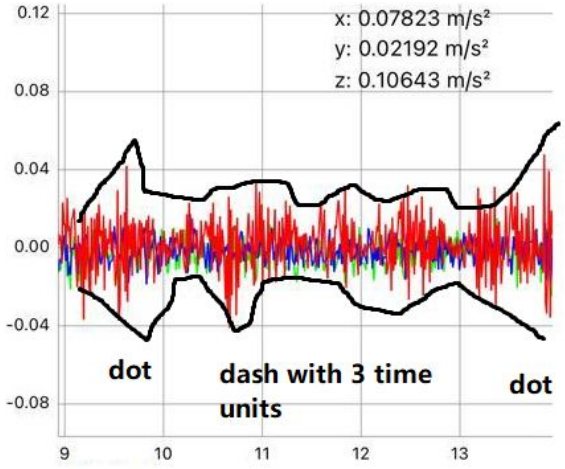
...



3 Testing and result
3.1 Traditional vs 1 & 0 Morse code

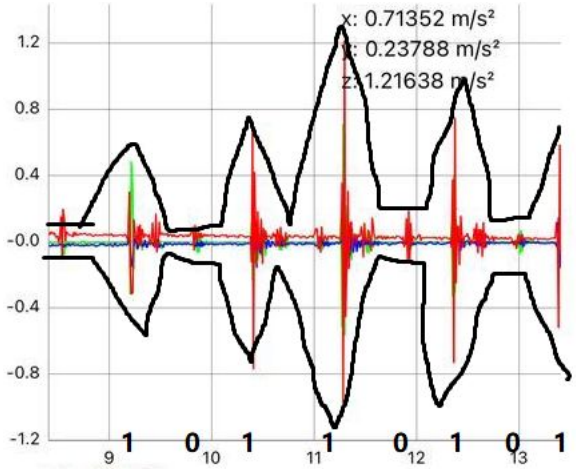
The 1 & 0 morse code can transfer data faster and clearer.

Traditional Morse code



...

1 & 0 Morse code



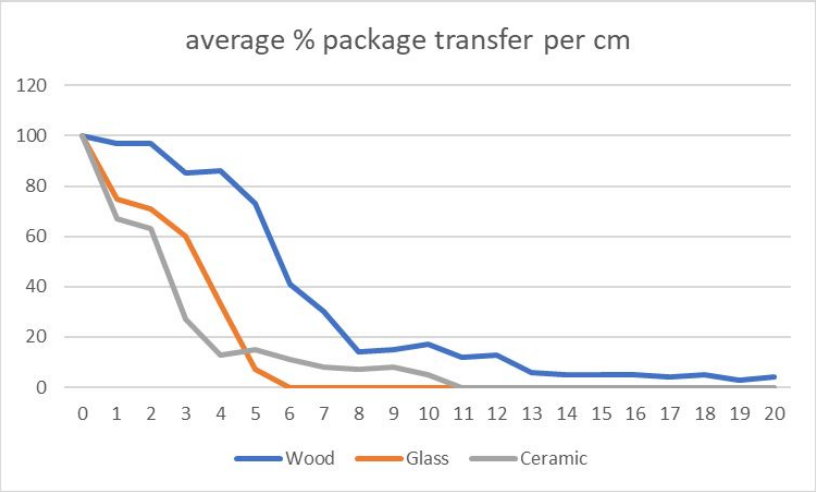
3 Testing and result
3.1 Medium and distance testing

In the testing, the difference of **acceleration speed** shows similar result.

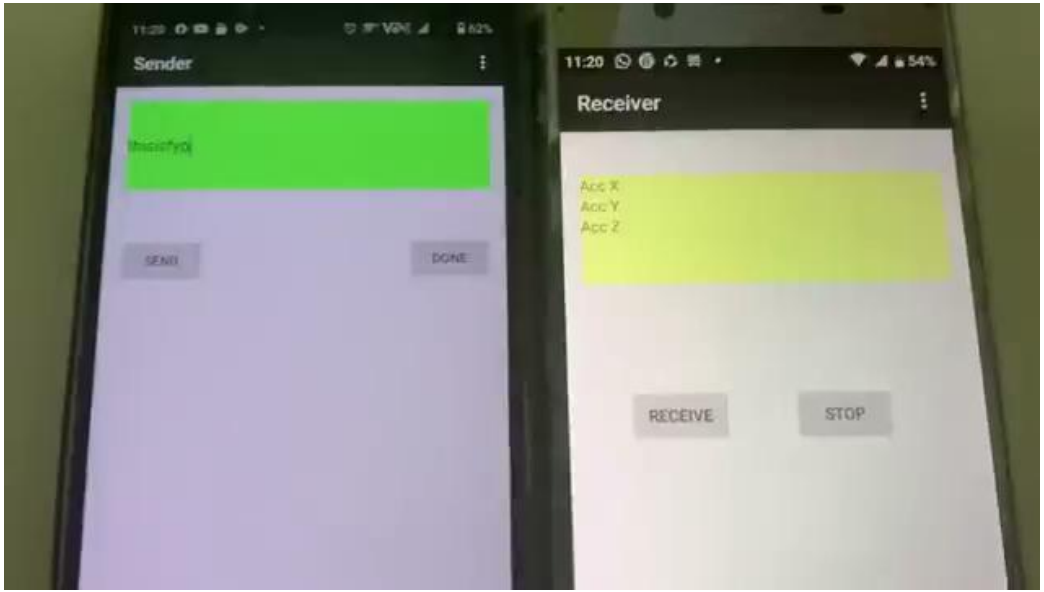
The **distance** will greatly affect the accuracy and completeness of messages transmission.

The best way is to put the **phones one on other and putting them side by side**.

...



3 Testing and result
3.1 Demo



Simplify LeaveHomeSafe scanning steps

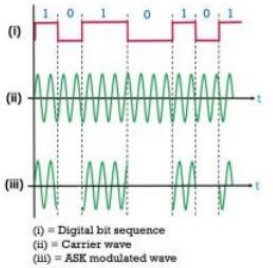
Messages can be transmitted in two-way one by one in short time. For example, a tablet or device can be install in restaurants to record visitors.

Smart Food Pager

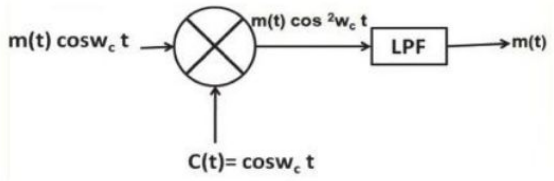
A new food pager with IMU and vobrators installed.

- Help Crowd Control
- Convenience
- Remote Sensing

3 Testing and result
3.2 Expectation



1 ASK MOD



ASK DEMOD 3

2

...

3 Testing and result
3.2 result

In the demodulation stage, noises from the environment are **unexpectedly significant** and the demodulation suffers from a **low success rate** even in quiet environments.

Considering the situation, the whole testing platform is changed to entirely using Matlab to simulate real-life situations.

...

3 Testing and result
3.2 Result

To test the performance of ASK in different amount of noises, 4 scenarios will be tested which are

(1) No noise interference

(2) Small amounts of noise (Eg. Library)

(3) Medium amounts of noise (Eg. Conversation)

(4) High amounts of noise (Eg. Construction site)

3 Testing and result
3.2 Result

The bits recovery rates = Recovered bits / Original number of bits of different scenarios

No noise interference	**100%**
Small amounts of noise	**100%**
Medium amounts of noise	**37.5%**
High amounts of noise	**0%**

04

Conclusion

4 Conclusion

What we have attempted

To develop an android application that is capable of vibrating in certain patterns and design a signal processing algorithm to modulate and demodulate signals by ASK.

What problem we have encountered

The physical interference from the real-world environment is unexpectedly significant which causes the shift of the testing platform.

...

4 Conclusion

What we have found out

ASK modulation method is proved to be capable of transmitting vibration signals with small amounts of noise with a 100% recovery rate but badly performing when it comes to medium or high amounts of noise.

...

4 Conclusion

We achieved:

- Wireless Radio-free Communication
- Secure Data Transmission
- Faster than traditional morse code
- Alternative method to QR-code

Difficulties:

- Unsuccessful in Long Distance
- Unstable in Long Message Transfer
- Cannot Reach Higher Transmission Rate

05

Future direction

5 Future direction

These two aspects are suggested to improve:

- ASK modulation optimizing:
  1) Physical filter
  2) Anti-noise signal
- Application adjustment:
  1) Strength of vibration
  2) Mismatch of bit stream frequencies

5 Future direction

- Room of improvement:
  1) Increase transmission distance
  2) Increase packet delivery rate
  3) Increase accuracy

- Other Security Implementation:

  1) ASCII code : replace Morse code to 8-bits binary and improve performance with more operations.
  2) Hash function

Thanks!

Do you have any questions?

Group number: Z2
Student 1: POON, Wai Hong, 1155125126
Student 2: MA, Yi Tsung, 1155125509
Supervisor: Prof. YAN, Zhenyu