Intelligent Access Control System Based on Acoustic Wave Communication

Yubing Jiang\(^1\), Huihong Shi, Xiaoli Hu, Hongwei Du and Liqin Zhou

College of Communication and Engineering, Jilin University, Changchun 130012, China

\(^{1}\)E-mail: jiangyb2016@mails.jlu.edu.cn

Abstract. In this paper, the mode to convey information of the modulated signal of the project is analyzed from the waveform of the modulated signal of binary amplitude modulation. Then the feasibility of the decoding rule adopted by the project is analyzed by using the knowledge of the only decodable information theory, which proves that as long as the intervals between the high level and between the codes are distinguished, it can be unlocked by transmitting the password information through the 10KHZ sound wave by counting the number of the intervals. Then, the acoustic wave signal receiving and processing circuit is designed. After going through the amplifying circuit, the filtering circuit and the shaping circuit, the sound wave signal can be converted into a door lock code to control the lock tongue drive module to unlock.

1. Introduction
With the improvement of science and technology and living standards, people's awareness of security is also constantly improving. With traditional mechanical key unlocking, people often need to carry multiple keys, which is not convenient enough. Therefore, it is an inevitable trend to replace the traditional mechanical password lock with a convenient and reliable electronic intelligent password lock. And with the development of large-scale integrated circuit technology and the improvement of communication principles, the password lock is developing intelligently in the positive direction. Therefore, it is especially important to develop an intelligent, convenient, safe and effective unlocking method.

At present, NFC smart card lock, Bluetooth smart lock, WiFi smart lock, fingerprint smart lock, face smart lock, iris smart lock and so on are more common. NFC smart locks not only have cards that are easy to be damaged, but also can only be used for unlocking at a very close distance. Even NFC cards and locks need to be in contact with each other, which limits the communication distance [1]; Bluetooth smart locks and WiFi smart locks use more steps. Compared with the sound wave lock, it is slightly cumbersome; the technical procedures such as fingerprint recognition, face recognition, and iris recognition are complicated, and the biological locks manufactured are expensive and cannot be well popularized. Acoustic communication has established a small closed-loop communication between mobile phone terminals and smart door locks, which achieves two-way authentication communication between the two, showing outstanding advantages in terms of usage scenarios, information interaction time, manufacturing cost and compatibility. [2] Sonic unlocking has the advantages of high security, high-speed communication, high
reliability, low cost, convenient use, low power consumption, etc. However, this method has high requirements for noise elimination.

At present, sonic communication has been widely used in iphone and android, involving data and file transmission, as well as payment and many other fields. Most of these transmission techniques use sound waves as handshake signals and then use wifi or other channels to transmit data. The receiver first establishes a wifi hotspot, and then sends the hotspot name through the sound wave. The sender decodes the wifi hotspot name after receiving the sound wave, then automatically links the hot spot and transmits the file, and the whole process does not require manual intervention. The core technology and difficulty of these programs is acoustic communication.

Currently, the applied acoustic wave communication mainly uses a single-frequency sound signal to encode data, and then plays these single-frequency sounds. After receiving the sound, the receiver recognizes the frequency and then decodes the data according to the frequency. For example, we can match the sine wave of 1500HZ to the number 1, the sine wave of 1600HZ corresponds to the number 2, and the sine wave of 1700HZ corresponds to the number 3. Then the digit string 3123 corresponds to a 4-segment sine wave. The receiver records the sound, analyzes the received sound, and recognizes the four-segment sine wave frequency of 1700HZ, 1500HZ, 1600HZ, and 1700HZ, and then looks up the codebook, and the decoded number is 3123.

This study proposes a sonic communication coding and receiving method that can be applied to intelligent unlocking, analyzes the principle of this communication method, and establishes a model that can be used for acoustic wave unlocking. The model uses sound wave to transmit information to reduce the influence of the noise on information reception.

Table 1. Abbreviation explanation

| Abbreviation | Explanation |
|--------------|-------------|
| 2ASK         | Binary Amplitude Keying |
| NFC          | Short distance wireless communication |

2. Acoustic communication model

2ASK is the basis of digital modulation. [3] According to the linear modulation principle, a 2ASK signal can be represented as a unipolar non-return-to-zero sequence multiplying a sinusoidal carrier[7]. The general expression of a 2ASK signal is:

$$S_{2ASK}(t) = \sum_{n} a_n g(t - nT_s) \cos(\omega_c t)$$

Where $g(t)$ is a rectangular pulse of duration $T_s$, and the value of $a_n$ obeys the following relationship:

$$a_n = \begin{cases} 0, & \text{Probability is } p \\ 1, & \text{Probability is } 1 - p \end{cases}$$

Then order

$$s(t) = \sum_{n} a_n g(t - nT_s)$$

Then

$$s_{2ASK}(t) = s(t) \cos(\omega_c t)$$
Inspired by 2ASK signal and information theory coding, the unlocking password is a number from zero to nine. Information is transmitted through different numbers of corresponding high levels. The number of high levels corresponding to the number is:

\[ n_m = \begin{cases} 10, & n_s = 0 \\ n_s, & n_s = 1,2,3,4,5,6,7,8,9 \end{cases} \]

(5)

In addition, when transmitting the complete password information sound wave, it is possible to distinguish the interval between the high level and the interval between the passwords by controlling different low level time. The item is set to a high-frequency duration of one password transmission with an interval of 10 sound waves; a low-level interval in the between of a high level in one bit of a password has a duration of 3 sound waves. The flat duration of low level between different bit codes is 6 sonic cycles. So the time it takes to pass a six-digit password is about:

\[ t = 10 \times \frac{1}{f} \times \sum_{n=1}^{6} n_m + 3 \times \frac{1}{f} \times \sum_{n=1}^{6} (n_m - 1) + 30 \times \frac{1}{f} \]

(6)

The maximum time it takes to pass a password when \( n_s = 0 \) is:

\[ t_{max} = 10 \times 0.001 \times 6 \times 10 + 3 \times 0.001 \times 6 \times 9 + 30 \times 0.001 = 0.792 \text{ ms} \]

(7)

| **Table 2.** Composition of acoustic signal information |
|-------------------------------------------------------|
| **Password start sign** | **First sonic password** | **Interval between passwords** | **Second sonic password** | **Interval between passwords** | **......** | **Sixth Sonic Password** | **Check Digit** | **Password end flag** |

**Figure 1.** 2ASK waveform diagram

**Figure 2.** Schematic diagram of the acoustic signal used in the project

3. Function and structure

The fundamental difference between digital door locks and traditional door locks featuring mechanical keys is the use of digital authentication. The digital communication system overcomes the shortcomings of poor security and anti-interference ability of the analog communication system, and uses error correction to improve the reliability of data transmission. The error correction coding technique can be used for channel coding to increase the reliability of transmission. Acoustic communication refers to encoding data into acoustic signals for transmission to achieve point-to-point and one-to-many close communication[4]. When communicating, the data transmitting end encodes the data into an acoustic signal, which is sent out.
through the speaker output, and the data receiving end turns on the recording device. The transmitted data is received, and then the received data is decoded into target data.

The innovation of this project uses mobile phone as the signal source, the sound wave is used as the cryptographic carrier and the sound wave of 10KHZ is selected. The sound wave of 10KHZ is within the sound frequency range that the mobile phone can emit, thus ensuring the feasibility of the scheme. Because the acoustic wave frequency is higher, the sounding time required to transmit the password is extremely short, and the volume of the unlocked sound wave is small. Also the propagation distance is relatively close, and it is not easy to be recognized by others, and the certain unlocking sound also ensures the user's experience of unlocking.

The sound wave lock researched by the project is mainly composed of mobile phone app sound wave signal part, the sound wave signal receiving circuit part, the stm32 single chip processing cryptographic signal hardware control part and the lock tongue drive module.

Figure 3. Schematic diagram of the process of transmitting information through acoustic signals

4. Acoustic signal receiving and processing circuit

The receiving circuit of this experiment is divided into three parts, the amplifying circuit, the filtering circuit and the shaping circuit. Through these three parts of the circuit, the segmented sine wave signal sent by the mobile phone is converted into a high-quality high-low level signal recognizable by the single-chip microcomputer, thereby realizing unlocking control. [5]

Figure 4. Receiving circuit diagram

4.1. Microphone parameters

The 6kHz~16kHz band controls the brightness, macro brightness and sharpness of the tone. Select 10KHz sound wave as the signal, which both has clear sound and corresponding frequency in the microphone head (see Table 2 for the parameters of the microphone). People are not very sensitive to the sound of the frequency. When the volume is not quite large, it is also very difficult to record the password on the recording device around.
Table 3. Parameters of the microphone used in the experiment

| Frequency          | Current Consumotion | S/N Ratio | Max input sound level |
|--------------------|---------------------|-----------|-----------------------|
| 50-16,000HZ        | Max.0.5mA           | More than 58DB | 110DB SPL           |

Figure 5. Typical Frequency Response Curve

Figure 6. Test Circuit

4.2. The amplifying circuit
The sound wave from the mobile phone will be attenuated after transmitting a certain distance, and a certain amplification of the received signal is needed. In this experiment, the phase proportional amplifier circuit is used, the input impedance and the input impedance of the op amp are equal, close to infinity. By calculating the parameters of the debugging circuit, the amplitude of the input signal is appropriately amplified.

Figure 7. The received acoustic signal is compared with the amplified signal of the amplifier

4.3. The filter circuit
The sound wave emitted by the mobile phone will be doped into the noise during the transmission process, and will be advanced after the amplifier circuit. In one step, this experiment uses an active bandpass
voltage controlled filter to filter the input signal. The experiment uses single-frequency signal for information transmission. The smaller the filter bandwidth is, the smaller the noise in the effective signal is. By calculating the parameters of the debugging circuit components, an active band-pass filter with a center frequency of 10KHZ and a bandwidth of 0.1KHZ is designed to reduce noise maximumly.

4.4. The shaping circuit
This experiment uses two single-limit comparators to convert the transmitted sinusoidal signal into a square wave signal. One of the comparators turns a signal portion larger than a positive voltage into a positive square wave signal, and the other comparator will convert the signal portion smaller than a certain negative voltage into a positive square wave signal, and then the two signals are merged into a continuous wave signal of positive value through three NAND gates. After the square wave signal is output, through the capacitor it becomes a continuous short sawtooth signal, and then passes through an integrating circuit. By adjusting the parameters of the integral circuit, the waveforms of each segment are clearly distinguished. Finally, after the NAND gate circuit, the signal changes to a high-low level. The input enters the MCU to implement the password setting and comparison and then unlock it.

5. Experiment results and error analysis
The mobile phone sends a six-digit password in a sonic manner according to the code-setting rules set by the project, and the received level information is transmitted to the single-chip microcomputer through the receiving circuit for processing. The password sound wave is sent by the mobile phone app and the received signal is displayed by the oscilloscope. The information of the password detected on the surface of the test results is the same as the transmitted password information. On the basis of this, the environmental noise is added and then repeated more tests. It is found that the password transmission rate is still low in the condition of big noise.

In order to test the reliability strength of the circuit, the error rate of the password which is received by the calculation circuit is calculated when the signal generator sends a sound wave with a signal-to-noise ratio of 60 db to 100 db. The false positive rates under different signal to noise ratios are shown in the figure. The misrecognition rate of the electronic anti-theft lock should not exceed 1% [4]. Since the misrecognition rate is less than 1%, it can be concluded that the unlocking method adopted by the acoustic wave lock is feasible, and the sound wave unlocking is reliable.
6. Conclusions
This study analyzes the feasibility of transmitting cryptographic information in counting numbers of the high level of 10KHZ single-frequency sound waves by using a binary amplitude modulation (2ASK) and a unique decodable tree diagram. The maximum time required for information is about 0.792s, which proves that the model unlocking is efficient. The sound signal is transmitted by the mobile phone app to verify the reliability of the acoustic wave receiving circuit designed by the project including amplification, filtering and shaping. When the signal-noise ratio is 60db-100db, the mis-delivery rate of the door lock password information is about 0.8%. The model is suitable for the signal-noise ratio condition of the ordinary family unlocking environment. The method of sound wave unlocking applied by the project is reasonable, efficient and accurate.

References
[1] Cao Junli, Wang Yuanyuan. Research on the Distribution of Chinese Shared Bicycle Patent[J]. Chinese inventions and patents, 2017, 14(09):8-13.
[2] Zhang Wei. Intelligent door lock system based on ultrasonic wave [J]. Science and Technology Communication, 2017, 9 (23): 126-131.
[3] Wumiti Yunus, Wang Liejun. Experimental design of 2ASK communication system based on acoustic wave[J]. China Educational Technology and Equipment, 2018(04):26-29.
[4] ZHU Yuqiong, YANG Hong, HU Shuang. Design of communication experiment system based on acoustic wave[J]. Equipment manufacturing technique, 2017(03):264-266.
[5] Ni Deke. Application of Multisim in the Teaching of Digital Circuit Logic Design[J]. Journal of Xi'an University of Posts and Telecommunications, 2011, 16(S1):90-92.
[6] Tan Ziyi. Comparison of electronic anti-theft lock standard GA374-2001 and ANSI/UL1034-2004 [J]. China Public Safety, 2013 (07): 217-219.
[7] Cao Xuehong. Information Theory and Coding [M]. Beijing: Tsinghua University Press, 2009. 34-37