Secure Data Transfer in Ambient Audio

Shanmugavel.D
Asst. Professor, Department of Computer Science, SMIT, Chennai, Tamilnadu, India.

Poovarasi.V
Department of Computer Science, SMIT, Chennai, Tamilnadu, India.

Revathi.K
Department of Computer Science, SMIT, Chennai, Tamilnadu, India.

Vidhya Lakshmi.S
Department of Computer Science, SMIT, Chennai, Tamilnadu, India.

Abstract – Data transferring plays a significant role in mobile application. This is largely affected by eavesdropping during the transmission, when the data is not encrypted. In this paper, we propose a secure communication channel among devices based on similar audio patterns. Features of ambient audio are used to generate small information between the devices. We explore a common audio-fingerprinting approach and account the noise in the derived fingerprints by applying error correcting codes. In secure data transfer in ambient audio, the sender device will send audio signals via its speaker and the receiver device uses microphone to receive the signals and decode the data from the sound wave. Phase key shifting scheme is used for data encryption and decryption. PSK is a digital modulation scheme that conveys data by changing, or modulating, the phase of a reference signal. Android based mobile system is used as a sender and receiver to demonstrate the concept. This kind of work can be used for short range communication without using a network like wifi, Bluetooth, etc. These schemes are useful in mobile applications like private information sharing, payment authentication, Near Field communication (NFC), etc.

Index Terms – Short range smart phone communication, audio fingerprinting, ambient audio.

1. INTRODUCTION

Short range communication helps to share a small amount of data to be transferred between two wireless electronic devices like mobile, laptop, etc. Short-range communication includes Near Field communication (NFC) and ambient audio have qualified many smart phone applications such as information sharing, connecting to multiple devices at a same time, etc. Emerged from the radio frequency identification (RFID) technology, NFC can enable the reliable low power communication between RadioFrequency-tags and readers. However, NFC requires Android and IOS and has been supported by only about a dozen of smart phone platforms on the market. Recent studies have given that Near Field Communication is concentrating on the security vulnerabilities such as eavesdropping and jamming. In addition, several types of active attacks such as data corruption, relay attack and man in the middle attack also have been exploited on NFC enabled portable devices.

Compared to the NFC, the features from the ambient audio are used to generate a small data between smart phones. Basically ambient audio assist to detect the sound which is present in the environment.

It just records all the sounds which are all nearer to the device using microphone and send the recorded sound to the Voice Activity Detection (VAD).VAD is a technique used in the speech processing must be able to detect the human speech in the presence of a range of very diverse types of acoustic background noise. As an alternative to NFC, VAD have been increasingly used for speech coding and speech rec- ogntion and it can also be used to make inactive some processes during the non-speech section of an audio session.

The purpose of introducing these secure data transfer in ambient audio application is to transfer the data between devices. This application will transfer the information to the several smart phones at the same time but it should contain this application and should be in particular range for communication. However the security provided to this android application describes a successful defense against eavesdropping vastly depends on the careful analysis of the attack scenarios and adopting suitable protection mechanisms based on the analysis. The audio fingerprinting is best known for its ability to link unlabeled audio to corresponding metadata, regardless of the audio format. Audio finger- printing or content based audio identification (CBID) systems will extract a perceptual digest of a piece of audio content, i.e. a fingerprint and store it in a memory.

2. RELATED WORK

Smart phone plays a vital role in data transferring. In existing system for data transferring, smart phone requires Sim card, network (Wi-Fi), Bluetooth, etc. Bluetooth does still offer a longer signal range for connecting during data communication and transfers. Bluetooth is also a NFC, but it can transfer to the range up to thirty feet. Bluetooth also works without presence of Sim card but it requires internet connection. NFC technology has taken advantage of this and can connect two devices quickly, then turn the signal over to Bluetooth so the owners can move further away without severing the connection.

There are so many android applications to transfer a data in the presence of Wi-Fi, Sim card.

A.Technical Feasibility

Technical feasibility evaluates the hardware requirements, software technology, available personnel etc., The software developed as a part of the system is to be incorporated along with different other modules to generate a consolidated system. The system can be made capable of handling all the transactions involved, thereby eliminating the need of any other software for the purpose. All we need is an Android mobile phone without any Sim or network and a computer with android development environment.

3. SYSTEM DESIGN

Our goal is to develop an android application which provides a way to transfer the data between the mobiles via sound in a air medium. The sender will provide their input data in speech to the mike of the smart phone. The mike will record the data and send it to the audio to text conversion tool. This tool will hand over the text to the Fast Fourier transform (FFT) algorithm and also displays the text in the sender screen. FFT will modify a signal from its original domain (often time or space) to a representation in the frequency domain. Here, FFT will alter the text to ASCII code. The generated ASCII code will be encrypted with prefixes and postfix code. Consider an example a data as “hello” which will converted to ASCII code as “01101000 01100101 01101100 01101100 01101111“and then code will attached with prefix and postfix code data.

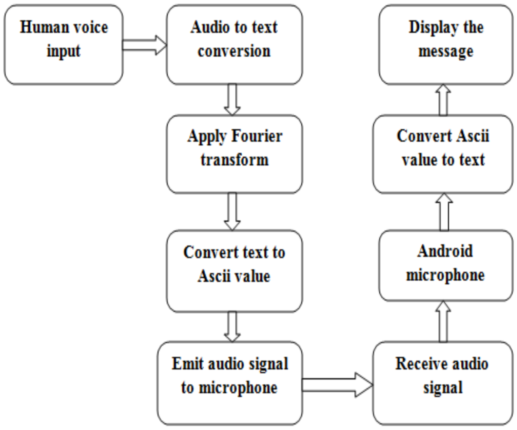

Fig 1. System Design

This data will be forwarded to the receiver in the form of sound signal through the air medium. The emitted sound signals are all captured by the microphone using ambient audio. Ambient audio will trace the entire sound signal which is available in the environment. Ambient audio uses VAD technique, to differentiate the information signal from the noise which is present in the sound signal. After the separation of information signal from noise, the signal will be send to the decryption process where prefix and postfix will be detached. Then at the receiver side, we use inverse FFT to convert the sound signal from frequency domain to its original domain i.e. ASCII code to original text format. Finally the sender text will be visible to the receiver on the smart phone screen. The Secure Data Transfer in Ambient Audio system work is splitted into four modules.

1. Give input data
2. Convert audio frequency
3. Transmitting audio
4. Receiving audio frequency

1. Give input data

The first module is to collect the input data; here the sender’s voice message will be recorded in the mike using audio to text conversion tool and displays the voice message as text in the screen.

2. Convert audio frequency

The second module is to convert the audio frequency, the input text will be converted to ASCII code and checks whether there is any error occurrence in the work.

3. Transmitting audio

The third module explains the process of transm- itting the audio frequency, here ASCII code will be encrypted with prefix and postfix code and then sound signal will be generated for the encrypted data from sender smart phone.

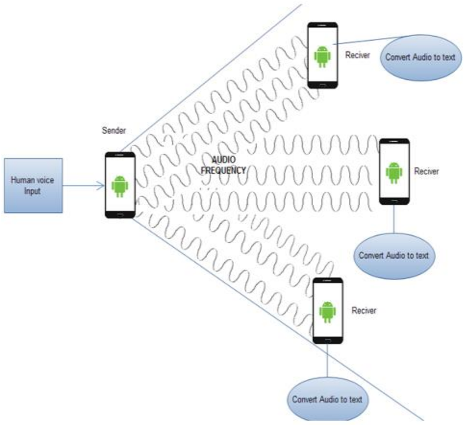

Fig 2. Functional Diagram

4. Receiving audio frequency

Finally in the fourth module, receiver will receive sound signal through microphone and applied the reverse process to the sound signal to obtain the original data which has been send from the sender and it will be visible to the receiver on the smart phone screen.

A.Security Model

Secure data transfer in Ambient Audio provides a successful defense against eaves- dropping vastly depends on careful analysis of the attack scenarios and adopting suitable protection mechanisms based on the analysis.

The possibilities of an eavesdropping are that the unauthorized person may capture the sound during audio transmission, but it is not possible to decrypt the information from the audio. On the other hand, the eavesdroppers can create an android application which is used to capture the sound signals while transmitting the data in air medium, but that application created by the eavesdroppers can view only the format of the data in symbol. At any cost, the information can't be decrypted by who are all not having this android application (Secure data Transfer in Ambient audio). Thus, the information transferred are protected from eavesdropping.

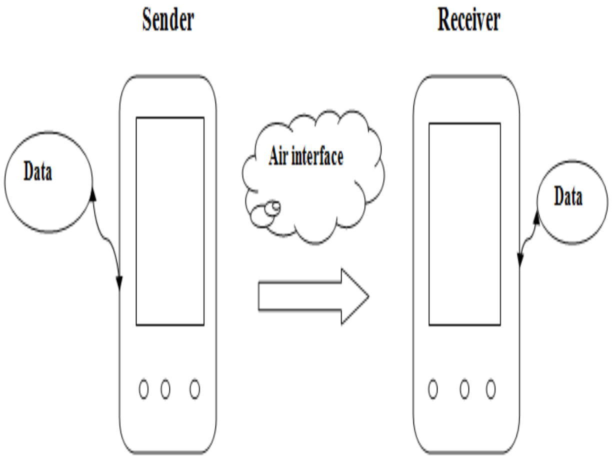

Fig 3. System Architecture

Hence, the distance factor is not considered into an account in our notion of visibility. The transmission rate decreases with the increase of the distance between the transmitter and the receiver .The data can be transferred in all direction i.e. 360°. However, similar to the distance factor in the case of NFC, it only offers a fuzzy security guarantee, because it is hard to make assumptions on the attackers' devices. For the sake of uniformity, we don't differentiate the visibility in terms of distance, which only increases the soundness of our security claim.

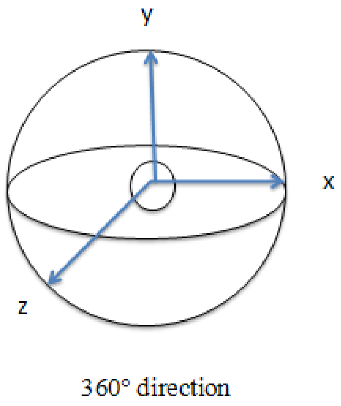

Fig 4. Data flow direction

B.Methodology

The methodology used here are Phase shift keying and Fast Fourier Transform. The Phase-shift keying (PSK) is a digital modulation scheme that conveys data by changing (modulating) the phase of a reference signal (the carrier wave). It is widely used for wireless LANs, RFID and Bluetooth commu- nication. Any digital modulation scheme uses a finite number of distinct signals to represent digital data. PSK uses a finite number of phases, each assigned a unique pattern of binary digits. Usually, each phase encrypts an equal number of bits. Each pattern of bits forms the symbol that is represented by the particular phase. They decrypt which is designed specifically for the symbol-set used by the modulator, determines the phase of the received signal and maps it back to the symbol it represents, thus recovering the original data.

4. FFT FRAMEWORK

A Fast Fourier Transform (FFT) algorithm calculates the discrete Fourier transform (DFT) of a sequence, or its inverse. The Fourier analysis helps us to convert a signal from its original form (often time and space) to a representation in the frequency domain and vice versa. An FFT rapidly computes the transformations by factorizing the DFT matrix into a product of sparse factors. An FFT will calculate the DFT and produces exactly the same result as evaluating the DFT process directly; but the most important difference is that an FFT is much faster(In the presence of round off error, many FFT algorithms are also much more accurate than evaluating in the DFT).

The best known FFT algorithm will depend on the factorization of N, but there are FFTs with O(N log N) complexity for all N, even prime N. Many FFT algorithms only depend on the fact that $e^{-\frac{2\pi i}{N}}$ is an N-th primitive root of unity, and thus can be applied to analogous transforms over any finite field, such as number-theoretic transforms.

Algorithm used

Algorithm 1:

```
FrameClassier(fpigN i=1 ; )
R = 0; B = 0;
For i   1 to N do
ifjjpi ‖prjj1 <then
R++;
ifjjpi ‖ pbjj1 <then
B++;
if R > 0 \ B = 0 then
Return ‘Red’;
else if B > 0 \ R = 0 then
Return ‘Blue’;
else
Return ‘None’;
```

Algorithm 2: Sender(M)

```
M1; : : : ;MnSplit(M);
fori 1 to ndo
whileNo NewAudiosampledetected do
Obtain audio sample;
Ridecode(NewAudioSample); Ci= Mi_ Ri;
Fi encode(Ci); display(Fi);
return?;
```

Algorithm 3: Receiver(_)

```
R1
$
f0; 1g`p ;F1 encode(R1); display(F1);
R2
$
f0; 1g`p ;F2 encode(R2);
fori 2 to n + 1 do
whileNo NewAudioSampledetected do
Obtain audio sample;
display(Fi);
Ci‖1 decode(NewAudioSample);
Mi‖1 = Ci‖1 _ Ri‖1;
ifi _ n then
Ri+1
$
f0; 1g`p ;Fi+1 encode(Ri+1);
returnM = M1jj : : : jjMn;
```

A.Comparsion Between NFC and Bluetooth

1.The main advantage is to transfer a data via sound in air medium without network connection, Bluetooth connection, even Sim card is not necessary.

2.NFC can connect to a distance about 4 centimeters but Bluetooth can connect to the devices about thirty feet.

3.NFC consumes less power than Bluetooth

4.NFC will face problems in close proximity of other connections but Bluetooth having trouble shooting to clear all these problems

5.NFC will act faster than Bluetooth.

5. CONCLUSION

Secure Data Transfer in Ambient Audio is evaluated through extensive experiments in Android smart phones, and the results show that our system achieves high level security and NFC-comparable throughput. The system can be used for private information sharing, secure device pairing and secure mobile payment, etc. To our best knowledge, this work is the first one that formally defines and studies the security of a smart phone system.

6. FUTURE ENHANCEMENT

The future enhancement for this project is to transfer data in long distance using ambient audio through air medium without any Sim card, Wi-Fi. This concept will help the user to communicate several users at a time.

REFERENCES

[1] Google, “Google Wallet,” URL: http://www.google.com/wallet/ index.html, accessed: 2013-01-01.

[2] S. Millward, “AliPay’s Mobile Barcode Payments in China,” URL: http://www.techinasia.com/alipay-mobile-payments/, accessed: 2013-01-01.

[3] R. Kim, “PayPal’s Barcode-based Payment Services in UK,” URL: http://gigaom.com/2012/05/30/ paypal-rolls-out-barcode-payments-in-the-uk.

[4] A. P. Jonathan M. Mccune and M. K. Reiter, “Seeing-is-believing: Using camera phones for human-verifiable authentication,” in In IEEE Symposium on Security and Privacy, 2005, pp. 110–124

[5] Nick Palmer A763896 ,”Audio fingerprinting”.URL:http://www.palmnet.me.uk/uni/FYP/Audio%20Fingerprinting.pdf

[6] Gilbert Strang described the FFT as "the most important numerical algorithm of our lifetime" and it was included in Top 10 Algorithms of 20th Century by the IEEE journal Computing in Science & Engineering.

[7] Cooley and Tukey published a more general version of FFT. URL: https://en.wikipedia.org/wiki/Fast_Fourier_transform.

[8] B. Zhang, K. Ren, G. Xing, X. Fu, and C. Wang, “SBVLC: secure barcode-based visible light communication for smartphones,” in IEEE Conference INFOCOM 2014, 2014, pp. 2661–2669.

[9] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, “Practical relay attack on contactless transactions by using nfc mobile phones,” ePrint Archive, Report 2011/618, 2011.

[10] M. Allah, “Strengths and weaknesses of near field communication (nfc) technology,” GJCST, vol. 11, no. 3, 2011.