INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

AMBIENT AUDIO BASED KEY GENERATION USING ASYNCHRONIZATION METHOD

Ms.S.Praveena[1], Mr P.S.Rajakumar[2]

[1]*M.TECH - Computer Systems and networks,, Dr.MGR Educational and Research Institute, Maduravoyal, Chennai 95, Tamil Nadu*[1]*jspraveena91@gmail.com*

[2]Associate Professor –Computer science and engineering, *Dr.MGR Educational and Research Institute, Maduravoyal, Chennai-95, Tamil Nadu* [2] *suraarus@yahoo.com,*

Abstract

We propose to establish a secure communication channel among devices based on similar audio patterns. Features from ambient audio are used to generate a shared cryptographic key between devices without exchanging information about the ambient audio itself or the features utilized for the key generation process. By Using Asynchronous method, Audio is recorded only in sender side Frequency is calculated from audio and it is converted into binary digits. Audio fingerprint is directly used as keys for an encryption scheme. The source node encrypts the information using the fingerprint and transfers the encrypted data and recorded audio to destination. The receiver must generate the fingerprint to decrypt the information from the received audio given by Source.

Keywords: — FFT, Ambient audio, Audio Finger print, Data encryption, Data decryption

1. Introduction

The mainstay of this project is to establish a secure communication channel among devices based on ambient audio patterns. Ambient audio are used to generate a shared cryptographic key between devices. This fuzzy-cryptography scheme enables the adaptation of a specific value for the tolerated noise among fingerprints based on environmental conditions by altering the parameters of the length of the audio samples utilized. We apply statistical tests to show that the entropy of fingerprints based on ambient audio is high. This fuzzy-cryptography scheme enables the adaptation of a specific value for the tolerated noise among fingerprints based on environmental conditions by altering the parameters of the error correction and the length of the audio samples utilized. In this paper, we experimentally verify the feasibility of the protocol in four different realistic settings and a laboratory experiment.

We establish an ad-hoc secure communication channel between unacquainted devices which is conditioned on the surrounding context. In particular, we consider audio as a source of spatially centered context. We exploit the similarity of features from ambient audio by devices in proximity to create a secure communication channel exclusively based on these features. At no point in the protocol the secret itself or information that could be used to derive audio feature values is made public. In order to do so, we generate audio fingerprints from ambient sounds. On each communicating device an identical key is generated.

2. System Analysis

The accelerometer of the Smart-It device to extract characteristic features from simultaneous shaking processes of two devices. An authentication mechanism based on this principle. They demonstrated that an authentication is possible when devices are shaken simultaneously by a single person, while an authentication was unlikely for a third person trying to mimic the correct movement pattern remotely. The proposed protocol that can be utilized with arbitrary context features repeatedly exchanges hashes of key-sub-sequences until a common secret is found. In this instrumentation, the fast Fourier transformation (FFT) coefficients of a sequence of accelerometer samples are utilized.

3. Synchronization

We establish an ad-hoc secure communication channel between unacquainted devices which is conditioned on the surrounding context. In particular, we consider audio as a source of spatially centered context. We exploit the similarity of features from ambient audio by devices in proximity to create a secure communication channel exclusively based on these features. At no point in the protocol the secret itself or information that could be used to derive audio feature values is made public. In order to do so, we generate audio fingerprints from ambient sounds. On each communicating device an identical key is generated

4. Implementation

4.1 Audio Capture

In a device Ambient audio was originated from individuals speaking in an Environment or Surroundings. The source captures the audio for generating the fingerprints and simultaneously transmits to the Destination.

4.2 Generating Audio Fingerprint

Audio-fingerprinting is an approach to derive a characteristic pattern from an audio sequence. The extraction of features from a piece of audio. These features are usually isolated in a time-frequency analysis after application of Fourier transforms. Discrete Fourier Transform (DFT) technique transforms one function into another function, which is called the Frequency Domain from Time Domain. From the Frequency of an particular audio the Fingerprints are generated. The audio-fingerprints directly used as keys for an encryption scheme. For an eavesdropper in a different audio context it shall be computationally infeasible to use any intercepted data to decrypt a message or parts of it.

4.3 Generating Audio Fingerprint Using Synchronization method

By using synchronization method audio is recorded in a certain time at sender and receiver side Frequency is calculated from audio and it is converted into binary digits using FFT .This binary digits is used as Audio Fingerprint for encrypting and decrypting a message

4.4 Generating Audio Fingerprint using Asynchronization method

In synchronization method, the frequency is varied based on the Distance. So same audio fingerprint cannot be generated. In Asynchronous method, Audio is recorded only in sender side Frequency is calculated from audio and it is converted into binary digits.

4.5 Encryption and Decryption using Audio Fingerprint

Audio fingerprint is directly used as keys for an encryption scheme. The source node encrypts the information using the fingerprint and transfers the encrypted data and recorded audio to destination. The receiver must generate the fingerprint to decrypt the information from the received audio given by Source.

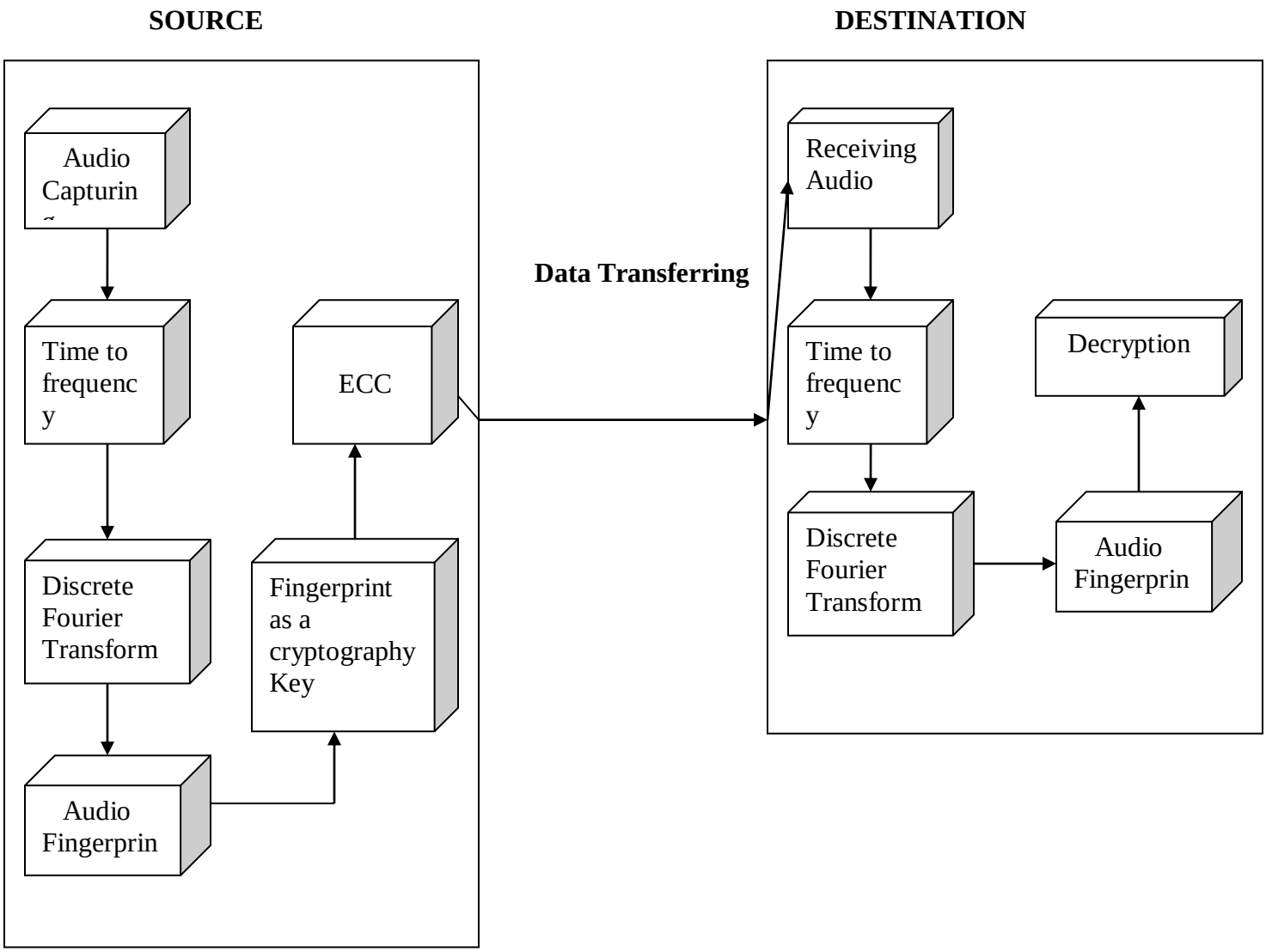

Figure 1: Architecture of Key Generating Process

5. Conclusion

In this paper we designed to establish a secure communication channel among devices based on ambient audio patterns through Generating Audio Finger print which is Characteristic pattern derived from audio. The source captures the audio for generating the fingerprints and simultaneously transmits to the Destination.

References

[1] C. Dupuy and A. Torre, Local Clusters, Trust, Confidence and Proximity, Series Clusters and Globalisation: The Development of Urban and Regional Economies, pp. 175-195, Edward Elgar, 2006.

[2] R. Mayrhofer and H. Gellersen, "Spontaneous Mobile Device Authentication Based on Sensor Data," Information Security Technical Report, vol. 13, no. 3, pp. 136-150, 2008.

[3] D. Bichler, G. Stromberg, M. Huemer, and M. Loew, "Key Generation Based on Acceleration Data of Shaking Processes," Proc. Ninth Int'l Conf. Ubiquitous Computing, J. Krumm, ed., 2007.

[4] L.E. Holmquist, F. Mattern, B. Schiele, P. Schiele, P. Alahuhta, M. Beigl, and H.W. Gellersen, "Smart-Its Friends: A Technique for Users to Easily Establish Connections Between Smart Artefacts," Proc. Third Int'l Conf. Ubiquitous Computing, 2001.

[5] A. Varshavsky, A. Scannell, A. LaMarca, and E. de Lara, "Amigo: Proximity-Based Authentication of Mobile Devices," Int'l J. Security and Networks, vol. 4, pp. 4-16, 2009.

[6] H.-W. Gellersen, G. Kortuem, A. Schmidt, and M. Beigl, "Physical Prototyping with Smart-Its," IEEE Pervasive Computing, vol. 4, pp. 10-18, 2004.

[7] R. Mayrhofer and H. Gellersen, "Shake Well Before Use: Authentication Based on Accelerometer Data," Proc. Fifth Int'l Conf. Pervasive Computing, pp. 144-161, 2007.

[8] R. Mayrhofer, "The Candidate Key Protocol for Generating Secret Shared Keys from Similar Sensor Data Streams," Proc. Fourth European Conf. Security and Privacy in Ad-Hoc and Sensor Networks, pp. 1-15, 2007.