ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Secure Communication Based Sound Transfer for Smart Phone

P.Periasamy [1], R.Rejeeth[2], V.Ganesh Kumar [3], Dr.K.Saravanan [4]

B.E Final year Student, Dept. of Computer Science and Engineering, Pavai College of Technology, Tamilnadu, India [1]

B.E Final year Student, Dept. of Computer Science and Engineering, Pavai College of Technology, Tamilnadu, India [2]

B.E Final year Student, Dept. of Computer Science and Engineering, Pavai College of Technology, Tamilnadu, India [3]

Associate Professor & Head, Dept. of CSE, Pavai College of Technology, Tamilnadu, India [4]

ABSTRACT: Secure Communication based message transfer mechanism in existing system uses Secure Barcode based Visible Light intensity to data transfer through visible light intensity in particular distance. Secure data embed in barcode and send light visible communication in these technologies lots of barcode reader read the information what embed in barcode. To overcome the drawbacks, we proposed a system message transfer through sound via digital analog signal in which users can given text in sender application, get that string to convert analog signal using Fourier transmission algorithm and original text encode to emit analog signal when receiver application enter that area automatically read wave signal to convert text and apply decode to display the original data.

I. INTRODUCTION

In a controlled environment we recorded several audio samples with two microphones placed at distinct positions in a laboratory. The samples were played back by a single audio source. Microphones were attached to the left and right ports of an audio card on a single computer with audio cables of equal lengths. They were placed at 1.5, 3,4.5, and 6 m distance to the audio source. For each setting, the two microphones were always located at non equal distances. In several experiments, the audio source emitted the samples at quiet, medium, and loud volume. The audio samples utilized consisted of several instances of music, a person clapping her hands, snapping her fingers, speaking, and whistling. Dependent on the specific sample, the meandB for these loudness levels varied slightly. The loudness levels for several sample classes experienced in 1.5 m

distance. For these samples recorded by both microphones we created audio fingerprints and compared their Hamming distances pair-wise. We distinguish between fingerprints created for audio sampled simultaneously and non simultaneously. Overall, 7,500 distinct comparisons between fingerprints are conducted in various environmental settings.

From these, 300 comparisons are created for simultaneously recorded samples. Simultaneously and Non simultaneously for several positions of the microphones and for several loudness levels. The error bars depict the variance in the Hamming distance. First, we observe that the similarity in the fingerprints is significantly higher for simultaneously sampled audio in all cases. Also, , the similarity in the fingerprints of Non simultaneously recorded audio is slightly higher than 50 percent, which we would expect for a random guess. The small deviation is a consequence of the monotonous electronic background noise originated by the recording devices consisting of the microphones and the audio chipsets. Additionally, the distance of the microphones to the audio source has no impact on the similarity of fingerprints. Similarly, we cannot observe a significant effect of the loudness level. This confirms our expectation since for the fingerprinting approach not the absolute energy on frequency bands but changes in energy over time were considered Therefore, changes in the loudness level as, for instance, by altering the distance to the audio source or by changing the volume of the audio, have minor impact on the fingerprints. All experiments. We observe that one of the comparisons of fingerprints for non simultaneously audio yielded a maximum similarity of 0.6484. This value is still fairly separated from the minimum bit similarity observed for fingerprints from simultaneously recorded samples. Also, this event is very seldom in the 7,200 comparisons since the mean is sharply concentrated around the median with a low variance. Therefore, by repeating this process for a small number of times, we reduce the probability

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

of such an event to a negligible value. For instance, only about 3.8 percent of the comparisons between fingerprints from non matching samples have a similarity of more than 0.58; only 0.4583 percent have a similarity of more than 0.6. Similarly, only 2.33 percent of the comparisons of synchronously sampled audio have a similarity of less than 0. 7.With these results, we conclude that an authentication based on audio fingerprints created from synchronized audio samples in identical environmental contexts is feasible. However, since it is unlikely that the fingerprints match in all bits, it is not possible to utilize the audio fingerprints directly as a secret key to establish a secure communication channel among devices. We therefore considered error correcting codes to account for the noise.

II. RELATED WORK

Contactless technology is widely used in security sensitive applications, including identification, payment and access-control systems. Near Field Communication (NFC) is a short-range contactless technology allowing mobile devices to act primarily as either a reader or a token. Relay attacks exploit the assumption that a contactless token within communication range is in close proximity, by placing a proxy-token in range of a contactless reader and relaying communication over a greater distance to a proxy-reader communicating with the authentic token. It has been theorised that NFC-enabled mobile phones could be used as a generic relay attack platform without any additional hardware, but this has not been successfully demonstrated in practice. We present a practical implementation of an NFC-enabled relay attack, requiring only suitable mobile software applications. This implementation reduces the complexity of relay attacks and therefore has potential security implications for current contactless systems. We also discuss countermeasures to mitigate the attack.

Radio Frequency Identification (RFID) technology has become increasingly prevalent in everyday applications. Contactless technology is a subset of RFID systems operating at 13.56 MHz, with an operating range of up to 10 cm. This technology comprises mature standards and industry specifications and is widely used by the smart card sector in security sensitive systems. Contactless technology is currently used in credit card payment, e-ID and e-passport systems, transport ticketing and access control systems. The practical security of contactless systems is therefore an active research area, both in terms of the actual channel and deployed applications.

III. EXISTING SYSTEM

Existing system uses the ambient audio which emits the audio frequencies which is acquired by the user who pass by the shopping mall or shop the product information is then acquired by the user in their mobile. Based on the product information he receives he decides whether to shop in that particular shop. But here we does not use encryption technique and uses few older encryption technique so the information can easily be acquired by the intruders. And the shop will be vulnerable.

Disadvantages

So this system is insecure because it is open to various types of attacks such as brute force attack, denial of service attack. The information they transmit to the user is not secured and which me acquired by the intruder.

IV. PROPOSED SCHEME OF WORK

Thus to overcome the disadvantages of existing model, we proposed a new system. With encryption technique ADHOC Based Audio Encryption. Fingerprint Based Authentication. Using these techniques the system will be secured and the user can get the secured audio frequency and decrypt the data and see the particular shops information and can decide to shop products from that shop. In an indoor Localized mall.

Advantages

As this system uses secured encryption techniques like Fingerprint Based Authentication to make the Communication secured in the system.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

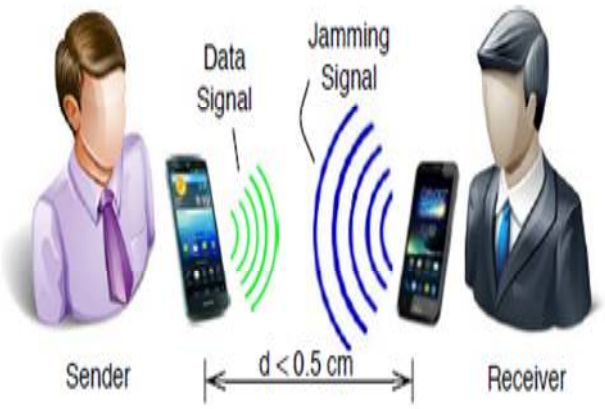

Fig 1: Proposed Architecture

V. ALGORITHM

Fast Fourier Transform Algorithm

The main purpose of this document is to provide a mathematical treatment of FFT algorithms, extending the work of fiducially and Bernstein. Many of the algorithms contained in this manuscript have appeared in the literature before, but not from this algebraic perspective. While it is unlikely that the completion of this thesis will trigger a revolution similar to that which followed the publication of the Cooley and Tukey paper, it is hoped that this document will help to popularize this mathematical perspective of FFT algorithms. Another purpose of the document is to introduce a new algorithm originally invented by Shuhong Gao that quickly evaluates a polynomial over special collections of finite field elements. Although it turned out that this algorithm is less efficient than existing techniques for all practical sizes, the careful study of the Cooley-Tukey algorithms through this research effort resulted in a new version of the algorithm that is superior to existing techniques for all practical sizes. The new version of this algorithm will also be introduced as part of this manuscript. We will then show how the new algorithm can be used to multiply polynomials with coefficients over a fi- nite field more efficiently than Sch¨onhage's algorithm, the most efficient polynomial multiplication algorithm for finite fields currently known. 2 Most FFT algorithms only work when the input size is the power of a small prime. This document will also introduce new algorithms that work for an arbitrary input size. We will then explore several applications of the FFT that can be improved using the new algorithms including polynomial division, the computation of the greatest common divisor, and decoding Reed-Solomon codes. Another motivation for writing this document is to provide a treatment of the FFT that takes the perspective of both mathematicians and engineers into account so that these two communities may better communicate with each other. The engineering perspective of the FFT has been briefly introduced in these opening remarks. We will now consider the mathematician's perspective of the FFT.

VI. METHODOLOGIES

Emitting audio frequencies of the shop information:

The audio frequencies are emitted by the shops in the indoor Localized shopping mall. 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

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

synchronized audio fingerprints from ambient sounds and utilize error correcting codes to account for noise in the feature vector. On each communicating device the feature vector is then used to create an identical key.

Audio Frequency Emitted Is Secured By Associating Encryption Techniques

The audio frequencies that are emitted by the associated shops uses the fingerprint based encryption technique to make the data communicated secured and safe. Audio Information indeed suffices to derive spatial information. They combine audio readings with accelerometer data to classify locations of mobile devices. In their work, the noise emitted by a vibrating mobile phone was utilized to distinguish among 35 specific locations in three different rooms with over 90 percent accuracy. Instead, we utilize purely ambient noise to establish a secure communication channel among devices in spatial proximity. We record NTP-synchronized audio samples at two locations, generate a characteristic audio fingerprint and map this fingerprint to a unique secret key with the help of error correcting codes.

Android Application to acquire the emitted secured ambient audio

We create an android application here to acquire the emitted data of a particular shop. The last step is necessary since the similarity between fingerprints is typically not sufficient to establish a secure channel. With fuzzy-cryptography schemes, the generation of an identical key based on noisy input data is possible. Li and Chang analyze the usage of biometric or multimedia data as part of an authentication process and propose a protocol. Due to the use of error-tolerant cryptographic techniques, this protocol is robust against noise in the input data. The authors utilize a secure sketch to produce public information about an input without revealing it. The input can then be recovered given another value that is close to it. A similar study is presented. The authors establish a key distribution based on a fuzzy vault using data measured by devices worn on the human body. The fuzzy vault scheme enables the decryption of a secret with any key that is substantially similar to the key used for encryption.

The Application decrypts the encrypted ambient audio

The android application then decrypts the received audio stream to read the information received of a particular shop and decides on shopping on that particular shop.

To use the audio fingerprints directly as keys for a classic encryption scheme the concurrence of fingerprints generated from related audio sequences has to be 1 with a considerably high probability. Since we experienced a substantial difference in the audio-fingerprints created we consider the application of fuzzy cryptography schemes. Note that a perfect match in fingerprints is unlikely since devices are spatially separated, not exactly synchronized and utilize possibly different audio hardware. The proposed cryptographic protocol shall be feasible unattended and ad hoc with unacquainted devices. 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. Additionally, we want to control the threshold for the tolerated offset between fingerprints based on contextual conditions of different physical locations.

VI. CONCLUSION

We have studied the feasibility to utilize contextual information to establish a secure communication channel among devices. The approach was exemplified for ambient audio and can be similarly applied to alternative features or context sources. The proposed fuzzy-cryptography scheme is adaptable in its noise tolerance through the parameters of the error correcting code utilized and the audio sample length. In a laboratory environment, we utilized sets of recordings for five situations at three loudness levels and four relative positions of microphones and audio source. We derived in 7,500 experiments the expected Hamming distance among audio fingerprints. The fraction of identical bits is above 0.75 for fingerprints from th e same audio context and below 0.55 otherwise. This gap in the Hamming distance can be exploited to generate a common secret among devices in the same audio context. We detailed a protocol utilizing fuzzy-cryptography schemes that does not require the transmission of any information on the secure key. The common secret is instead conditioned on fingerprints from synchronized audio recordings. The scheme enables ad hoc and unobtrusive generation of a secure channel among devices in the same context. We conducted a set of common statistical tests and showed that the entropy of audio fingerprints based on energy differences in adjacent frequency

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

bands is high and sufficient to implement a cryptographic scheme. In four case studies, we verified the feasibility of the protocol under realistic conditions. The greatest separation between fingerprints from identical and non identical audio contexts was observed indoor with low background noise and a single dominant audio source. In such an environment, we could distinguish devices in the same and in different audio contexts. It was even possible to clearly identify a device that replicated dominant audio from another room with an equally tuned FM-radio at similar loudness level. In a case study conducted in a crowded canteen environment, we observed that the synchronization quality was generally impaired due to the absence of a dominant audio source. However, it was still possible to establish a privacy area of about 2 m inside which the Hamming distance of fingerprints was distinguishably smaller than for greater distances. The worst results have been obtained in a setting conducted beside a heavily trafficked road. In this case, when the noise component becomes dominant and considerably louder, the synchronization quality was further reduced. Additionally, due to the increased loudness level, a similar synchronization quality was possible also at distances of about 9 m. We conclude that in this scenario, a secure communication channel based purely on ambient audio is hard to establish.

VII. FUTURE WORK

We claim that the synchronization quality in scenarios with more dominant noise components can be further improved with improved features and fingerprint algorithms. Currently, most ideas are lent from fingerprinting algorithms and features designed to distinguish between music sequences. Although algorithms have been adapted to better capture characteristics of ambient audio, we believe that features and fingerprint generation to classify ambient audio might be further improved. Additionally, the consideration of additional contextual features such as light or RF-channel-based should improve the robustness of the presented approach. In our implementation we faced difficulties to achieve sufficiently accurate (in the order of few milliseconds) time synchronization among wireless devices. In our current studies, we tested several sample windows of NTP-synchronized recordings in order to achieve a feasible implementation on standard hardware. However, a more exact time synchronization would further reduce the accuracy and computational complexity of the approach.

REFERENCES

[1] 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.
[2] M. Allah, "Strengths and weaknesses of near field communication (nfc) technology," GJCST, vol. 11, no. 3, 2011.
[3] T. Langlotz and O. Bimber, "Unsynchronized 4d barcodes: coding and decoding time-multiplexed 2d colorcodes," in ISVC, 2007.
[4] T. Hao, R. Zhou, and G. Xing, "Cobra: color barcode streaming for smartphone systems," in MobiSys, 2012.
[5] J. H˚astad, R. Impagliazzo, L. Levin, and M. Luby, "Construction of a pseudo-random generator from any one-way function," SIAM Journal on Computing, vol. 28, pp. 12–24, 1993.
[6] D. Parikh and G. Jancke, "Localization and segmentation of a 2d high capacity color barcode," in WACV, 2008.
[7] S. Perli, N. Ahmed, and D. Katabi, "Pixnet: interference-free wireless links using lcd-camera pairs," in MobiCom, 2010.
[8] J. McCune, A. Perrig, and M. Reiter, "Seeing-Is-Believing: using camera phones for human-verifiable authentication," Int. J. Secur. Netw., vol. 4, no. 1/2, pp. 43–56, 2009.
[9] N. Saxena, J. erik Ekberg, K. Kostiainen, and N. Asokan, "Secure device pairing based on a visual channel," in S & P, 2006.
[10] R. Kainda, I. Flechais, and A. W. Roscoe, "Usability and security of out of-band channels in secure device pairing protocols," in Symposium on Usable Privacy and Security (SOUPS'09). ACM, 2009, pp.11:1–11:12.