Cryptographic Key Generation based on Contextual Information: A Review

Aparna A.
P G Scholar
Department of Computer Science & Engineering
College of Engineering, Perumon(CUSAT), Kerala, India

Ajish S.
Assistant Professor in CSE
Department of Computer Science & Engineering
College of Engineering, Perumon(CUSAT), Kerala, India

ABSTRACT

With the capabilities of computing increasing by leaps and bounds, the need for trusted communication also rises. The present state of ensuring secure communication between devices largely relies on the use of cryptographic keys. The primitive and advanced key generation strategies involve the use of password only, biometric, quantum, PRNG technologies. Recently, the use of contextual information to generate highly secure keys has proven to be a realistic and unobstructed method in the field of cryptography. Contextual information like temperature, luminance and ambient audio may be used for this purpose. This paper presents a detailed survey on the cryptographic techniques for key generation based on contextual information. A brief comparison on the current techniques is also presented in this survey.

General Terms

Cryptography, Feature Extraction, Key Generation

Keywords

Contextual Information, Key Generation, Data Encryption, Ambient Audio, Audio Fingerprinting

1. INTRODUCTION

With the increased number of penetration attempts by mobile devices in the recent years, the need for achieving a secure channel between communicating devices has been proven to be one of the most important requirements in the field of security. It is hard to accomplish secure mobile communication among unacquainted devices due to the demand of an immune authentication process between them. Authentication between the communicating partners can be brought about by the establishment of a shared cryptographic key[7], which can be generated as per the selection of different frameworks for cryptographic key generation. Encrypting the actual message with a cryptographic key ensures that the communication is actually conducted with the intended recipient and not with a malicious third party entity.

Nowadays there exist a number of techniques for key generation. One of the most widely used and the simplest method is the password authentication technique. Advanced techniques include biometric key generation, pseudorandom number generator, and quantum cryptographic key generation. The biometric key generation methodology focuses on the extraction and combination of biometric features of users such as iris, fingerprint, and face with a predefined salt. The resultant hash of the combination does not contain any important secrets of the user. The pseudorandom number generator works on the random generation of a number sequence, which would then be used as the cryptographic key for the communication that follows. On the other hand, quantum cryptography extracts the features of light and has its roots on certain assumptions in physics. The result of a quantum cryptographic key generator is a highly secure and robust cryptographic key.

Studies conducted over the recent years point that security of mobile devices has elevated to be one of the trending research discussions today. Researchers desire much more of an un-obstructive system for establishing a secure channel between the communicating devices. One of the core concepts is that the number of communicating participants as well as the communication range should never be underestimated. A device pairing paradigm capable of providing an un-obstructive security based on environmental contexts in particular mobile devices that are equipped with a multitude of sensors. The sensors equipped in the devices help in the detection of different environmental stimuli such as audio, light, RF channel, temperature or proximity.

Using contextual information for key generation proves to be an un-obstructive and realistic approach which handles with the real context of the communication environment. Current techniques of audio cryptography are capable of increasing the security to a much higher level by considering the perceptual features of the audio present in the concerned environment. It is evident that the ambient audio under consideration tolerates a certain amount of noise[12]. The calculation of fingerprints by taking into account the energy difference between perceptual peaks of ambient audio results in highly secure cryptographic keys having high entropy and that are immune to guessing. The disadvantages of the biometric approach is as follows:

(1) Only a restricted amount of biometric samples are available and hence limited availability of biometric information.
(2) The security provided by biometric data can be broken by a determined adversary by taking high quality photographs of an Iris or face.
(3) Biometric data can't be changed significantly. In order to increase the burden for an adversary to break a security system,

it is beneficial to periodically change the secret utilized. If we use biometric features for security, this requirement cannot be met.

Quantum cryptography also relies on the aspect of contextual information. Quantum emulation is infeasible due to the requirement of expensive quantum computer. Audio as a context for key generation never requires an additional or change in the existing infrastructure. The rest of this paper discusses a comparative study of the different strategies used for context based cryptography. This paper reviews most of the methodologies that involve feature extraction from ambient audio.

2. SURVEY ON CONTEXT BASED KEY GENERATION

The greatest challenge in mobile device pairing for information transfer is the authentication of participant devices. During the pairing process, it is difficult to validate the intended mobile device to which the sender wants to communicate.

2.1 Ambient audio based secure mobile phone communication

Ngu Nguyen et al., 2012, [1] proposed an un-obstructive mechanisms to establish synchronization between devices based on the environmental audio for secure key generation. With the help of inbuilt microphones, each mobile device willing to communicate capture synchronized audio samples from the environment that are needed to establish a common key. Each device then extracts the perceptual features of the recorded audio and then computes a binary characteristic sequence[8]. This sequence is unique for each of the captured audio samples along with the surrounding noise and hence known by the name audio fingerprint.

This unique binary code is designed to fall on to a code-space of an error correcting code. In general, a fingerprint will not match in every respect with any other fingerprint that is generated from the same environment due to the presence of noise. In the considered context, audio is spatially centered at particular instants. Fingerprints generated from similar ambient audio are more or less similar, but due to noise and inaccuracy in the audio sampling process, it is unlikely that two fingerprints are flawlessly identical. Devices utilize their error codes for mapping fingerprints to the corresponding code words. The fingerprints having a hamming distance within a predefined threshold corresponds to identical code words and is then considered as secure keys[11]. The hamming distance between the fingerprints is directly proportional to the distance between devices.

Secure device pairing based on audio is one of the most important applications. People can connect mobile devices just by keeping their devices in close proximity. The connection process does not cause any hindrance to their functionalities.

2.2 Pattern-based alignment of audio data for ad hoc secure device pairing

Sigg, S et al., 2012, [2] constructed an Ad hoc Pairing application, which is an audio based secure system for Android mobile devices. It utilizes the concepts of Fuzzy cryptography. Synchronization in audio samples is achieved with the help of an approximate pattern matching which is independent of device communication. The solutions for establishing a secure communication key between unacquainted devices require explicit user input to provide a shared piece of information. Devices which are willing to communicate are placed at a distance d from an audio source. Each device records ten audio samples. The creation of fingerprints begins with the detection of the top 10 matching positions of a common pattern extracted from each audio sequence. Each device can function either as a sender or a receiver. As a result, each device can have 10 keys. Senders use these keys for encrypting the original data block, and on the other side the corresponding receiver use the key with best matching result for decryption purposes. In case the attempt for decryption fails, the receiver can use the next top similar key, and this process is continued for 10 trails until the decryption process is successful[10]. The entropy investigation of the 512 bit fingerprint results in the production of a P value, which reveals that the fingerprints generated from recorded ambient audio are unbiased. For creating fingerprints, the audio sequence is divided into n frames, each of which is then processed with FFT. The system split the result into m non overlapping frequency bands of width:

$$b = \frac{maxfreq(S_i) - minfreq(S_i)}{m}$$

Afterwards, binary fingerprints are created by comparing energy fluctuation in successive frames as,

$$f(i,j) = \begin{cases} 1, (E(i,j)E(i,j+1)E(i-1,j)E(i-1,j+1)) > 0 \\ 0, otherwise \end{cases}$$

2.3 Pintext : A framework for secure communication based on context

Stephan Sigg et al., 2012, [3] proposed a framework for device pairing based on contextual information. Mobile devices have inbuilt sensors that detect environmental stimuli such as audio, light, RF, temperature and proximity. A secure communication channel based on common but arbitrary contextual classes temperature, light and audio is depicted as follows in Figure-1,

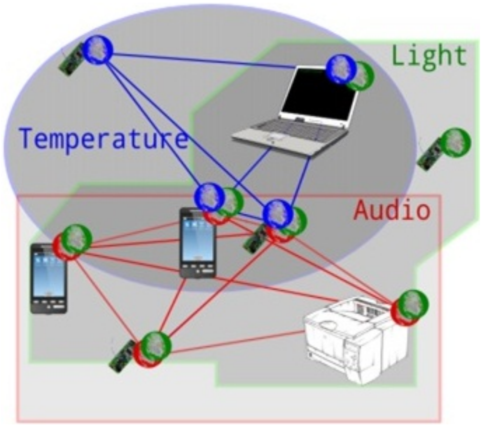

Fig. 1. Contextual information for secure key generation

For instance, the communication between two laptops situated in the same audio context cannot be overheard by a third party entity present in another audio context[9]. It is also possible to take light as contextual information, but it may be shared by a large number of devices simultaneously and hence a loss in secrecy is unavoidable. A framework for context based device authentication consists of mainly five modules and are depicted in Figure-2::

Device Synchronization: The system desires synchronization among devices for sharing a common secret without any fluctuation based on considered context. This module establishes sufficient synchronization dependent on the accuracy required.

Feature Extraction: The current contextual features are extracted using a feature extraction method.

Context Processing: Preprocessing techniques like smoothing and noise removal are applied on the extracted features.

Key Generation: Using the compact notation of extracted feature representation, a key is generated. For enhancing the security and robustness it can be incorporated with any of the error correction mechanism and can be mapped to corresponding code words.

Communication: The generated secure key is used for safe encrypted communication.

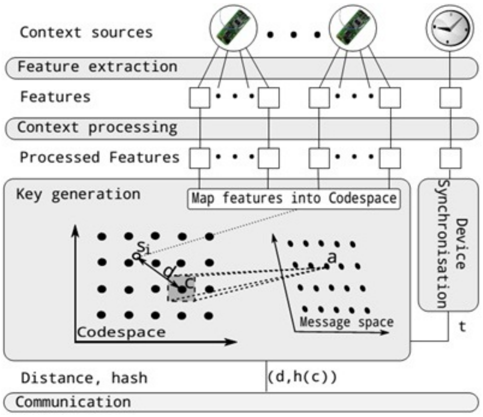

Fig. 2. Modules of Device-Pairing Framework

2.4 Key Generation Approach to Encrypt Wireless Communication using RF Channel

Bichler D et al., 2007, [4] demonstrated that an RF Channel can serve as a device authentication mechanism. The channel property is spatially centered and is not predictable at any of the remote location. In the absence of an interference, both the transmitter as well as the receiver experiences identical channel responses. It is based on this information that the establishment of a secure key among a node pair is done.

System provides effective security for data communication by assigning standard algorithms for both encryption and decryption. The source information is generated by a key pad and will be encrypted is sent to destination through RF communication. The receiving system will check the data and decrypt the corresponding encrypted message.

2.5 Key Generation Based on Acceleration Data of Shaking Processes

Guido Stromberg et al., 2007, [5] proposed a system and proved that it is also possible to analyze the accelerometer reading provides a measure of the amount of shaking of the devices. The extraction of characteristic features from simultaneous shaking processes is extremely difficult, since it requires repeated hash exchanges of key-sub-sequences until a common secret found.

The fingerprints generated by the participating devices are affected by the presence of noise or interference. The Error Correction Code technique is applied since it tolerates a specific amount of noise in fingerprints. A secure communication established between devices by shaking them together. Instead of distributing or exchanging a key, the devices independently generate a key from the measured acceleration data by appropriate signal processing methods.

2.6 Proximate: proximity-based secure pairing using ambient wireless signals

Suhas Mathur et al., 2011, [6] Both the sender and the target can easily observe a typical laser beam (light). With the aid of high speed cameras, it is possible to capture the modulated signals with enough accuracy, which can be used to generate a secret key among willing devices for a spontaneous device authentication.

Forming secure associations between wireless devices that do not share a prior trust relationship is an important problem. Temporal variations in the wireless RF channel from a public source (Peter) can be used by parties in physical proximity (Alice and Bob) to extract a random cryptographic key. An adversary (Eve) who is not within the proximity of Alice and Bob cannot extract the same key.

3. COMPARISON OF CONTEXTUAL KEY GENERATION TECHNIQUES

Depending upon various contextual information utilized each of the above described papers should be subjected to some comparative study, especially by means of error tolerance rate. Ngu Nguyen et al., 2012, [1] proposed audio fingerprint generation scheme just from two devices keeping them in close proximity. Scheme utilizes ambient audio as the context and chance for error rate is comparatively high. Chance for error is very low while using RF channel properties utilized, since the channel behavior is highly unique. Table-1 depicts a comparative analysis based on error tolerance rate.

Table 1. Comparison of Techniques

Basis of Procedure	Context	Error Tolerance Rate
Connect mobile devices just by keeping them in close proximity, audio fingerprints generated from surrounding audio context.	Ambient Audio	Low
Fingerprints created by the detection of the top 10 matching positions of a common pattern extracted from each audio sequence.	Ambient Audio	Medium
Framework based on common but arbitrary contextual classes temperature, light and audio.	Temperature, light and audio	Depends on the context
Utilized the RF Channel property for key generation.	RF Channel	High
The amount of shaking of the devices is measured by an accelerometer which is subsequently used for key generation	Shaking	Medium
The properties of a laser beam are analysed for key generation.	Light	Medium

A comparison analysis based on error tolerance rate is shown in the following chart.

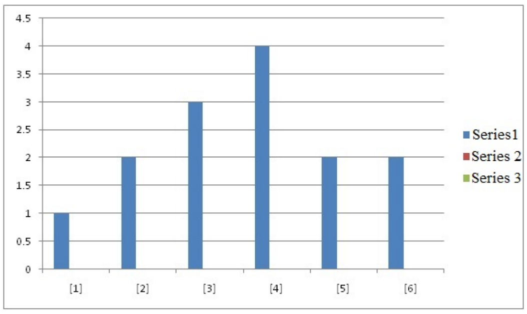

Fig. 3. Comparison chart

4. EXPERIMENTAL RESULTS AND ANALYSIS

4.1 Experimental Results of Ambient audio based secure mobile phone communication

Eventhough the system could dynamically adapt the secure communication between mobile phones based on ambient audio, the experimental results proved that:

—The hamming distance between the fingerprints is directly proportional to the distance between devices.

4.2 Experimental Results of Pattern-based alignment of audio data for ad hoc secure device pairing

Synchronization in audio samples is achieved with the help of an approximate pattern matching which is independent of device communication.

—Each device can have 10 keys.

—Possibility of guessing keys is less.

—Decryption is only possible with the best matching key among the 10 keys.

4.3 Experimental Results of Pintext

The evaluation results of [3] revealed the following areas:

—The channel property is spatially centered and is not predictable at any of the remote location.

—Mobile devices have inbuilt sensors that detect environmental stimuli such as audio, light, RF, temperature and proximity.

—A framework for context based device authentication consists of mainly five modules

4.4 Experimental Results of Key Generation Approach using RF Channel

The evaluation results of [4] revealed the following areas:

—There exists a framework for device pairing based on contextual information.

—System provides effective security for data communication by assigning standard algorithms for both encryption and decryption.

—The source information is generated by a key pad and will be encrypted is sent to destination through RF communication.

4.5 Experimental Analysis of Key Generation Based on Acceleration Data of Shaking Processes

The evaluation results of [5] revealed the following areas:

—Requires repeated hash exchanges of key-sub-sequences until a common secret found.

—The Error Correction Code technique is applied since it tolerates a specific amount of noise in fingerprints.

4.6 Experimental Analysis of Proximate

The evaluation results of [6] revealed the following areas:

—With the aid of high speed cameras, it is possible to capture the modulated signals with enough accuracy.

—Used to generate a secret key among willing devices for a spontaneous device authentication.

4.7 Experimental Analysis of Context Based Key Generation Method

The experimental results are visualized in following chart based on the pattern matching approach for context based key generation.

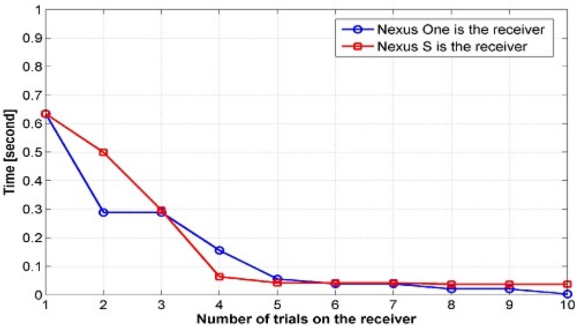

Fig. 4. Comparison chart

5. CONCLUSION

A secure communication channel among devices is established by utilizing the freely available contextual information. Various contexts as ambient audio, light can be used for secure key generation by devices which equipped with sensors. The approach was exemplified for ambient audio and can be similarly applied to alternative contexts. In this paper, some of the techniques that make use of the contextual information to generate a safe and secure key are reviewed. Additionally, an analysis of the properties of fingerprints was presented and estimated the entropy in statistical tests.

6. REFERENCES

[1] Ngu Nguyen, Stephan Sigg, An Huynh, and Yusheng Ji, "Using ambient audio in secure mobile phone communication", International Conference on Pervasive Computing and Communications, pp. 431-434, 2012

[2] Nguyen, Ngu, et al. "Pattern-based alignment of audio data for ad hoc secure device pairing", Wearable Computers (ISWC), 2012 16th International Symposium on. IEEE, pp. 88-91, 2012.

[3] Sigg, Stephan, Dominik Schuermann, and Yusheng Ji. "Pintext: A framework for secure communication based on context", Mobile and ubiquitous systems: Computing, networking, and services. Springer Berlin Heidelberg, pp. 314-325, 2012.

[4] D. Bichler, G. Stromberg, and M. Huemer, "Innovative Key Generation Approach to Encrypt Wireless Communication in Personal Area Networks", Proc. IEEE GlobeCom, pp. 177-181, 2007.

[5] D. Bichler, G. Stromberg, M. Huemer, and M. Loew, "Key Generation Based on Acceleration Data of Shaking Processes", Proc. Ninth Intl Conf. Ubiquitous Computing, J. Krumm, ed., pp. 304-317, 2007.

[6] Mathur, Suhas, et al. "Proximate: proximity-based secure pairing using ambient wireless signals." Proceedings of the 9th international conference on Mobile systems, applications, and services. ACM, pp. 211-224, 2011.

[7] Amresh Nikam, Poonam Kapade, Sonali Patil,"Audio Cryptography: A(2,2) Secret Sharing for Wave File",International Journal of Computer Science and Application Issue 2010.

[8] Alex Varshavsky,Anthony LaMarca,Eyal de Lara,"Enabling Secure and Spontaneous Communication between Mobile Devices using Common Radio Environment",Eighth IEEE Workshop on Mobile Computing Systems and Applications.

[9] Stephan Sigg, Matthias Budde, Yusheng Ji, Michael Beigl,"Entropy of audio fingerprints for unobtrusive device authentication",International and Interdisciplinary Conference on Modeling and Using Context 2011.

[10] Ngu Nguyen and Stephan Sigg, An Huynh, Yusheng Ji,"Pattern-based Alignment of Audio Data for Ad-hoc Secure Device Pairing",2012 16th International Symposium on Wearable Computers.

[11] Ngu Nguyen, Stephan Sigg, An Huynh, Yusheng Ji,"Using ambient audio in secure mobile phone communication",Work in Progress session at PerCom 2012, Lugano (19-23 March 2012),National Institute of Informatics (NII).

[12] Raviraj B. Vyavahare, Amit J. Bajaj, Hitesh P. Fuse, Mr. Pravin K. Patil,"Study of Secure Data Transmission Using Audio File",International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 2, February 2015.