Volume 3, No. 8, August 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICLE
Available Online at www.jgrcs.info

APPLICATIONS OF FUZZY ERROR CORRECTION IN COMMUNICATION SECURITY IN CRYPTOGRAPHY

Akshay Kumar Tyagi[1*],D.B.Ojha[2*]

[*1] Research Scholar Mewar University, Chittorgarh, Rajasthan
akshaytyagi@airtelmail.in

[*2] Department of Science & Technology, Mewar University, Rajasthan, India
ojhabrat@gmail.com

***Abstract*:** This paper discusses the applications of fuzzy error correction in communication security. Without a doubt the cryptography has become a very popular field of computer science. In fact, there are numerous techniques of cryptography that are used for securing a wide variety of applications. At the present, cryptography is also used to secure communication networks. This paper outlines the applications of such techniques that can be used to secure communication networks.

INTRODUCTION

The techniques of Cryptography conventionally depend on consistently distributed random data and information strings to deal with its special and secret data. Actuality this method makes it hard to generate, store, and constantly retrieve similar strings. In this scenario, strings that are neither consistently random nor consistently reproducible appear to be extra abundant. For instance common person's fingerprint or eye scan is obviously not a consistent random string, nor does it have imitated exactly every time it is measured (Dodis, Reyzin and Smith; Boyen).

Nowadays the communication and collaboration networks are evolving and offering an excellent support for business, corporate, educational purposes. However, threats regarding information security and privacy are also evolving and cause serious dangers for effective information security management. In this scenario, a number of security and privacy management solutions are available. This research presents an idea for the better management of network communication security and privacy. This basic purpose of this paper is to summarize the applications of fuzzy error correction in communication security in cryptography.

FUZZY CRYPTOGRAPHY

Frequently, one would desire to make use of various cryptographic equipments with estimated, noisy, and non-uniformly disseminated keys, rather than the exact, sternly random strings that are typically needed. Similarly "fuzzy" secret could be assessed on somewhat concealed biometric characteristics a retinal scan rather than a thumbprint. For instance, it could be a long password incorrectly dedicated to memory, or one's impulsive reactions to a list of personal questions. If at all possible, someone would be looking for a wide variety of techniques to alter some of the above into cryptographically powerful keys practical for a variety of purposes. Hence, a number of structures geared toward precise applications have surfaced in the previous few years (Dodis, Reyzin and Smith; Boyen).

The application of fuzzy cryptography can offer an excellent support for potential enhancement of network communication error correction and security. It is an admitted fact that the application of next generation security mechanisms has offered much better support and network security which have improved the security of a communication network.

PROBLEM DEFINITION

With the evolution of penetration through mobile devices in current years, safety and privacy threats as well as security necessities correspondingly have multiplied. In fact, it has augmented a wide variety of threats, though, is indistinct to wireless networks and mobile users as security methods are supposed as a hassle for the reason that they are not inconspicuous as well as might divert from high-level jobs (Boyen; Dodis, Reyzin and Smith; Al-saggaf and Acharya). The basic purpose of this research is to assess the application of fuzzy cryptography for achieving feasible network security and offering better security means that are less unobtrusive or even obtrusive?

PROPOSED SOLUTION

For the application of better security through fuzzy cryptography, the proposed idea is to make use of context (sensor generated, state reliant content for example ambient audio, location or ambient light) as an embedded method to implement a fundamental level of privacy and security. In fact, this context can be employed as frequent secret codes amongst devices in the similar circumstances. In this scenario, a major obstacle is that context is a noisy network communication source of information and data. Hence, there should be an effective way to deal with this noise are necessary. Another issue and challenge is to implement a framework illustration through adequately high entropy (Boyen; Dodis, Reyzin and Smith; Al-saggaf and Acharya).

CONTEXT-BASED DEVICE PAIRING WITH FUZZY CRYPTOGRAPHY

The proposed implementation of the fuzzy cryptography systems for mobile communication network is aimed

supporting and improving inconspicuously pair mobile systems foundational upon the environmental data and information. This research will assess a variety of environmental influences for example, audio or light for protecting ad-hoc network communication systems pairing. In this scenario, some of the present algorithm for present job will be modified as well as optimized to these functional inputs. As well, the entropy of the input information and data utilized will be researched for this project. The objective of this research is to propose an application that displays the device communication and pairing method on mobile based communication networks. In this scenario, (Sigg, Budde and Ji) have outlined the fundamental functionality of such system that is previously applied as well as tested as python code (Sigg, Budde and Ji; Al-saggaf and Acharya).

CONCLUSION

At the present, the use of cryptography techniques for securing communication networks has become very common. This paper has presented a brief overview of some of the important aspects of the fuzzy logic with respect to its application for the communication networks. This research has covered various ideas in the context of "applications of Fuzzy Error Correction in Communication Security in Cryptography". I hope this paper will offer a better idea of research we are going to perform.

WORKS CITED

Al-saggaf, Alawi A. and H. S. Acharya. A FUZZY COMMITMENT SCHEME. 2009. 29 August 2012 <http://arxiv.org/ftp/arxiv/papers/0809/0809.1318.pdf>.

Boyen, Xavier. "Reusable Cryptographic Fuzzy Extractors." CCS. Washington, DC, USA: ACM, 2004.

Dodis, Yevgeniy, Leonid Reyzin and Adam Smith. Fuzzy Extractors and Cryptography, or How to Use Your Fingerprints. 11 November 2003. 30 August 2012 <http://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/FuzzyExtractors.pdf>.

Sigg, Stephan, et al. Entropy of audio fingerprints for unobtrusive device authentication. 2011. 30 August 2012 <http://www.teco.edu/~budde/publications/CONTEXT2011_Sigg.pdfhttp://www.teco.edu/~budde/publications/CONTEXT2011_Sigg.pdf>.

Short Bio Data for the Author

AkshayKumar Tyagi, PersuingPh.D from MewarUniversity, Chittorgarh, Rajsthan, INDIA. He has more than fifteene year experience in IT & Academics Worked As HOD IT at Gradute School of Business & Administration, Greater Noida, U.P., INDIA. The current research area is Cryptography& fuzzy commitment scheme.

Dr. Deo Brat Ojha, Ph.D from Department of Applied Mathematics, Institute of Technology, Banaras Hindu University, Varansi (U.P.), INDIA in 2004. His research field is Optimization Techniques, Functional Analysis & Cryptography. He has more than Six year teaching & more than eight year research experience. He is working as a Professor at Mewar Institute of Technology, Ghaziabad (U.P.), INDIA.Dr. Ojha is the member of Mathematical Society Banaras Hindu University, LMIAENG, LMIACSIT. He is the author/co-author of more than 50 publications in International/National journals and conferences.

