

{tag}

{/tag}

IJCA Proceedings on International Conference
on Innovations in Computing Techniques (ICICT 2015)

© 2015 by IJCA Journal

ICICT 2015 - Number 1

Year of Publication: 2015

Authors:

R. Rekha

R. Vidhyapriya

R. Geetha Rajakumari

{bibtex}icict1472.bib{/bibtex}

Abstract

Wireless Body Sensor Network (WBSN) is an emerging technology in the area of telemedicine. It helps doctors to remotely monitor the health condition of patients. The success of usage of WBSNs for health care monitoring relies mainly on the security provided to the private information collected by the sensors. Security depends on key agreement scheme used. This paper aims at developing a fuzzy based key agreement scheme that uses ECG signal to

protect the symmetric key to be exchanged. Here the correlation attack is overcome by using two different polynomial of different order due to which the integrity property of system is preserved. The effectiveness of the proposed scheme is to improve the performance of the system by overcoming correlation and collusion attacks. It also aims at minimizing False Acceptance Rate (FAR) and False Rejection Rate (FRR).

References

ences

- Venkatasubramanian. K. K, Banerjee. A and Gupta. S. K. S, "PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks", IEEE Transactions on Information Technology in Biomedicine, Vol. 14, No. 1, January 2010.
- Sriram Cherukuri, Krishna K Venkatasubramanian , Sandeep K S Gupta , "BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body", IEEE International Conference on Parallel Processing, 2003.
- Ari Juels and Madhu Sudan. A Fuzzy Vault Scheme. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), page 408, 2002.
- T. Charles Clancy, Negar Kiyavash, and Dennis J. Lin. Secure Smartcard-Based Fingerprint Authentication. In Proceedings of the ACM SIGMM Workshop on Biometrics Methods and Applications, pages 45-52, Berkley, California, 2003.
- Umut Uludag, Sharath Pankanti, and Anil K. Jain. Fuzzy Vault for Fingerprints. In Proceedings of the Audio- and Video-based Biometric Person Authentication pages 310-319, Hilton Rye Town, USA, 2005.
- S. Yang and I. Verbauwhede. Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme. In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing pages 609-612, Philadelphia, USA, 2005.
- Ee-Chien Chang, Ren Shen, and Francis Weijian Teo. Finding the Original Point Set Hidden among Chaff. In Proceedings of the ACM Symposium on Information, Computer and Communications Security pages 182-188, 2006.
- Ee-Chien Chang and Qiming Li. Hiding Secret Points Amidst Chaff. In Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 59-72, Petersburg, Russia, 2006.
- Preda Mihailescu. The Fuzzy Vault for Fingerprints is Vulnerable to Brute Force Attack. W. L. W. AlTarawneh and W. L. Woo. Biometric Key Capsulation Technique Based on Fingerprint Vault: Anatomy and Attack. In Proceedings of the International Conference on Information and Communication Technologies: From Theory to Applications, pages 1-5, Syria, 2008.
- Karthik Nandakumar, Abhishek Nagar, and Anil K. Jain. Hardening Fingerprint Fuzzy Vault Using Password. In Proceedings of the International Conference on Biometrics, pages 927-937, Seoul, Korea, 2007.

Index Terms

Computer Science

Security

Keywords

Physiological Signals Key Agreement Fuzzy Vault Scheme.