VOL. 10, NO. 18, OCTOBER 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

128 BIT KEY GENERATIONS FROM THE DYNAMIC BEHAVIOR OF ECG FOR SECURING WIRELESS BODY AREA NETWORK

J. Mohana[1] and V. Thulasi Bai[2]
[1]Department of ECE, Saveetha University, Chennai, India
[2]Department of ECE, Prathyusha Institute of Technology and Management, Chennai, India
E-Mail: mohanajaishankar1@gmail.com

ABSTRACT

Wireless Body Area Network (WBAN) consists of resource constraints sensors and hence security methods with less computation are chosen. To make the resource consumption less, available information in the WBAN that is common to all the sensors is utilized. The proposed biometric security scheme is based on the distinctiveness and non-stationary behaviours of the ECG signal. This behaviour guarantees that the key generated for each individual is different. ECG also possesses the added advantage of generating keys with low latency that is a short duration of measured signal is enough. The above scheme reduces the need for the distribution of security key. The number of keys required by each node for secure communication is also reduced. The design constraints such as energy and randomness are considered in this work. In this research, the dynamic feature (i.e. ECG) is utilized to generate the key. The 128 bit key is generated from the R-R interval of the ECG signal. The generated 128 bit can be used as encryption keys in WBAN. The generated key shows randomness and distinctiveness.

Keywords: ECG, WBAN, cryptography.

INTRODUCTION

Rapid growth in Wireless Sensor Technology has increased the ability of easy and fast computing. The wireless sensors are connected to form Wireless Sensor Network (WSN). The most important application of Wireless Sensor Networks (WSN) is for healthcare application which includes the telemedicine. WSN that is used for healthcare application is called as Wireless Biomedical Area Network (WBAN). WBAN consists of sensors which are recognized as Biomedical Sensors. Improvements in sensors encompass the construction of small and lightweight biomedical sensors. Sensors such as electrocardiogram (ECG] sensors, pH value sensors pulse oximeters are worn on the individuals and the physiological data is measured. The measured value is communicated wirelessly to the base station from the human body. This has removed the usual way of wired communication between the biomedical sensors on the individual's body to a nearby monitoring system. The advantages of wireless communication are comfortability, flexibility and portability. The recent technique to enable secure communication in WBAN is Biometrics, where the physiological characteristics or behavioural qualities are used to provide authentication between the communicating entities. The body itself is used for managing cryptography keys between the nodes and the base station. The sensed value is used to generate a pseudo- random number which is same on both the sides. Next it is applied to encrypt and decrypt the data to be communicated. The physiological value for key generation should be chosen such that it exhibit time variance and randomness. ECG (electrocardiogram) proves to be appropriate for the above cause. The work reported in this paper bases its work on the idea of uniqueness and quasi-stationary characteristics of ECG signals. The rest of the paper is organized as follows. The related work is given in Section 2. In Section 3, the proposed algorithm for the 128-bit key generation is presented. In Section 4, the performance analysis of the proposed algorithm is described. Finally, conclusions are reported in Section 5.

RELATED WORK

Keys for symmetric crypto-systems are generated using standard key generating functions Cryptographic Random Numbers Standard (1995). These functions use pseudo random numbers as input parameters to generate unique keys. These functions are commonly known and hence the strength of the key generated depends upon the pseudo-random number. Any pseudo-random number irrespective of the source from which it is generated, it should satisfy certain conditions for them to be used for security purposes. This characteristic is known as cryptographic randomness. A random number generated from a particular source is said the cryptographically random, if it is not possible for an adversary with full knowledge of the working of the system to determine the number generated from the knowledge of previous numbers generated from the same source with a probability greater than half. This property ensures that the random number and hence the keys generated from it cannot be guessed by an adversary. In case of ordinary devices the pseudo-random number is generated from the hardware level and the key is generated at one node and is distributed to all the other nodes. This method is adopted because it is not possible to generate the same pseudo-random number at different nodes due to the differences in the hardware of the node. The conventional and generic sensor networks do not take into consideration the

environment in which they operate. Hence they do not attempt to make use of any resources which it may offer. If we could design architectures such that the sensors can make use of the surroundings in their computing tasks, then it would lead to significant advantages. Cherukuri *et al*. (2003) proposed using a group of similar random numbers generated from properties obtained from different human body parts to protect the transmission of symmetric keys between communicating parties. The transmitting node binds a cryptographic key with a locally captured biometric trait. At the receiving node, a binding-off process is preceded using the biometric trait captured by its own to recovery the cryptographic key. It was discussed in Poon *et al.* (2006) that biometric traits used in such a security model must be: 1) distinctive, i.e., the trait should be sufficiently different on any two individuals when copies of it are captured simultaneously, even if the copies are captured by different types of sensors and at different locations of the body and 2) time-variant but invulnerable, i.e., the trait should change with time and have a high degree of randomness so that copies of it captured at different times would not match even if they are obtained from the same individual. More importantly, from a cryptographic perspective, devices outside of a particular BSN have neither access to, nor can they reliably predict a particular period record of such a biometric trait. In Shu-Di Bao *et al*. (2008) based on the characteristics of IPIs, a lightweight generation scheme of EIs is proposed. Individual randomness and group similarity of the generated EIs are then evaluated. Motivated by this research, the dynamic feature (i.e. ECG) is utilized to generate the key. The interval between R-to-R (R-R) is utilized to generate the key based on dynamic biometric features (i.e. ECG). The performance of the key generated by the proposed algorithm is analysed in terms of design goals of randomness and distinctiveness.

PROPOSED METHODOLOGY

In this research, the dynamic feature (i.e. ECG) is utilized to generate the key. The interval between R-to-R (R-R) is utilized to generate the key based on dynamic biometric features (i.e. ECG). The secure communication of data is made so, as there is a possibility of modification and injection of these perceptive data. The security in Body Area Network (BAN) is classified into two categories, namely, authentication and data encryption. The network authentication is performed between various biosensor and Control Units (CU). Since there is a possibility of false authentication (i.e. attacker act as a true or original node) the second level of security (i.e. data encryption) is initiated. The encryption of the patient data is also an important process in securing the data on Body Area Network (BAN).The long-established cryptosystem usually follows two approaches, namely, the Token based approach and the Knowledge based approach. These approaches are limited as they can be stolen, duplicated or lost. Also the critical problem with these approaches is that uniqueness (i.e. unique user) cannot represent these approaches. In contrast to this, the approach based on biometric characteristics can support the uniqueness of the user. In tradition, the biometric features used in cryptography are face, iris and fingerprint. These characteristic are static in nature and even have the possibilities of getting tracked. To overcome the limitation of static biometric, biometric features such as an Electrocardiogram (ECG), Photo plethysmogram (PPG) are introduced for non-static (i.e. dynamic) biometric characteristics [1].

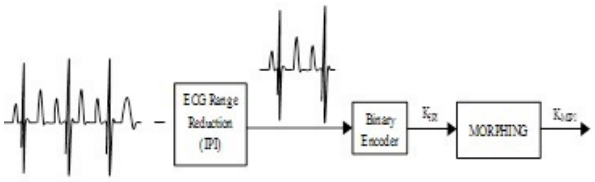

Figure-1. Key generation.

The algorithm used is as follows. Two different samples are taken. One sample ranges from 1 to 9 and it is converted from integer to string. Second sample from 1 to 6 with 64 bit key is stored in another variable. Both converted values are stored in Key matrix. The distance between the minimum and maximum value with 128 bit value is calculated. The XOR Value for the distance found in the previous step using ran dint function is calculated. From the above step (Random value) the 128 bit key is generated with 32 bit value. The generated key is converted into the matrix format. The resulted key is tested for randomness and distinctiveness which are the performance metrics of a cryptography key.

PERFORMANCE ANALYSIS

In this research the performance of the key generated by the proposed algorithm is analysed in terms of design goals of randomness and distinctiveness. The ECG data is obtained from 31 subjects obtained from the MIT Physio Bank database (http://www.physionet.org/physiobank/). The algorithm implementation and analysis was done using MATLAB. The Key A and Key B denote the keys generated by sensors s1 and s2 (located in the same BSN).

RANDOMNESS

It is also necessary to ensure that the keys generated are random enough to ensure that they are unpredictable. To validate this entropy of the keys generated for each individual is computed. It is found in the Figure-2 that in all cases the entropy values were close to 1, which shows that the distribution of 1s and 0s in the key is uniform. This result guarantees the randomness.

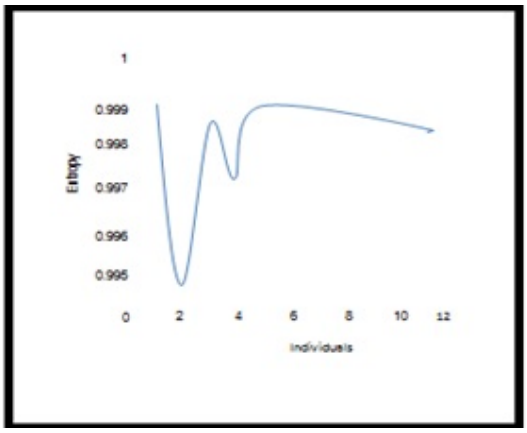

Figure-2. Entropy for different keys generated for different individuals.

DISTINCTIVENESS

The aim was to determine if the keys generated by the proposed algorithm are same for the same individuals and different for two different individuals. The average hamming distance between keys was calculated. Figure-3 shows the result at a random start time. The x-axis represents Key A of all individuals and y-axis represents Key B for all individuals. The colors symbolize the range within which the actual hamming distance between the two keys falls. In the figure all the diagonal values are zero. This proves that the keys generated from the ECG signals of the same individual are identical, while keys from two different individuals are different. This satisfies the design goal of distinctive.

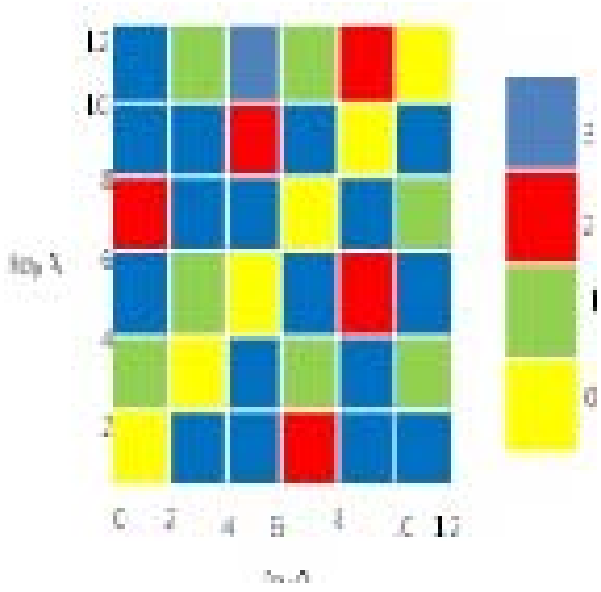

Figure-3. Hamming distance between keys generated for different individuals.

CONCLUSIONS

The chapter explores the randomness and distinctiveness of the generated 128 bit cryptography key from the R-R interval of ECG for securing the inter sensor communication in WBAN. The generated key can be used for any encryption algorithm.

REFERENCES

[1] Goldberger AL, Amaral LAN, Glass L, Hausdorff JM IvanovPCh, Mark RG, Mietus JE, Moody GB, Peng CK, Stanley HE. PhysioBank, Physio Toolkit and Physio Net: Components of a New Research Resource for Complex Physiologic Signals. Circulation. 101(23): e215-e220.

[2] S. Cherukuri, K. Venkatasubramanian and S. K. S. Gupta. 2003. BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body. 432-439, In Proc. Of Wireless Security and Privacy Workshop.

[3] C. Y. Poon, Y. T.Zhang and S. D. Bao. 2006. A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health. IEEE Communications Magazine. 44(4): 73-81.

[4] Bao SD, Poon CCY, Shen LF, Zhang YT. 2008. Using the timing information of heartbeats as an entity identifier to secure body sensor network. IEEE Transactions on Information Technology in Biomedicine. 12: 772-779.

[5] http://physionet.org/physiobank/database/.

[6] Cavoukian A, Stoianov. 2007. A. Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy. Information and Privacy Commissioner/Ontario.

[7] S. C. Saxena, A. Sharma and S. C. Chaudhary. 1997. Data compression and feature extraction of ECG signals. International Journal of Systems Science. 28(5): 483-498.

[8] Emran M. Tamil, Nor Hafeezah Kamarudin, Rosli Salleh, M. Yamani Idna Idris, Noorzaily M. Noor and Azmi Mohd Tamil. Heartbeat Electrocardiogram (ECG) Signal Feature Extraction Using Discrete Wavelet Transforms (DWT).

[9] L. Eschenauer and V. D. Gligor. 2002. A Key-Management Scheme for Distributed Sensor Networks. pp. 41-47, In Proc. Of the 9th ACM conference on Computer and Communications Security.

[10] S. D. Bao, Y. T. Zhang and Y.-T. Zhang. 2005. Physiological Signal Based Entity Authentication for

Body Area Sensor Networks and Mobile Healthcare Systems. pp. 2455-2458, In Proc. of the IEEE 27th Conference on Engineering in Medicine and Biology.

[11] 1995. Cryptographic Random Numbers Standard P1363: Appendix E.

[12] 2000. http://circ.ahajournals.org/cgi/content/full/101/23/e215.

[13] K. K. Venkatasubramanian, A. Banerjee and S. K. S. Gupta. 2008. EKG based key agreement in body sensor networks. In Proc. 27th Conf. Comput. Commun. (IEEE INFOCOM Workshops), Phoenix, AZ. pp. 1-6.

[14] M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux. 2011. On the security of oscillator-based random number generators. J. Cryptol. 24(2): 398-425.

[15] G. Blakley, D. Chaum, R. Fairfield, R. Mortenson and K. Coulthart. 1985. An LSI random number generator (RNG). In Advances in Cryptology. Berlin, Germany: Springer. pp. 203-230.

[16] G. H. Zhang, C. C. Y. Poon and Y. T. Zhang. 2010. A fast key generation method to secure body sensor networks for health applications. In Proc. IEEE 32nd Annu. Int. Conf. Eng. Med. Biol. Soc., Buenos Aires, Argentina. pp. 2034-2036.