31st Annual International Conference of the IEEE EMBS
Minneapolis, Minnesota, USA, September 2-6, 2009

A Biometric Method to Secure Telemedicine Systems

G. H. Zhang, Carmen C. Y. Poon, Member, IEEE, Ye. Li, *and* Y. T. Zhang, *Fellow, IEEE*

***Abstract*—Security and privacy are among the most crucial issues for data transmission in telemedicine systems. This paper proposes a solution for securing wireless data transmission in telemedicine systems, i.e. within a body sensor network (BSN), between the BSN and server as well as between the server and professionals who have assess to the server. A unique feature of this solution is the generation of random keys by physiological data (i.e. a biometric approach) for securing communication at all 3 levels. In the performance analysis, inter-pulse interval of photoplethysmogram is used as an example to generate these biometric keys to protect wireless data transmission. The results of statistical analysis and computational complexity suggest that this type of key is random enough to make telemedicine systems resistant to attacks.**

I. Introduction

When telemedicine was first proposed in the early 1970s, its function was often limited to offer medical consultation services [1]. The concept of telemedicine can be defined as using various telecommunications to provide health care or medical information and services to patients by physicians and medical institutions [2], [3]. Security of telemedicine systems is particularly important because sensitive medical information must be protected from unauthorized personnel for personal advantages and fraudulent acts.

The security of data transmission must be considered at all three levels for the telemedicine system with architecture as shown in Fig. 1 [4]: Communication within the body sensor network (BSN), from the BSN to the remote server and from the remote server to the professionals. First, biomedical sensors worn on or implanted in the same human body make up a wireless short-range BSN, which can collect real-time physiological data, such as blood pressure, heart rate, electrocardiogram (ECG), photoplethysmogram (PPG), etc.

Manuscript received April 23, 2009.

G. H. Zhang is with Institute of Computing Technology, Chinese Academy of Sciences, Graduate University of Chinese Academy of Sciences and CAS/CUHK Research Center for Biosensors and Medical Instruments, Institute of Biomedical and Health Engineering, Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, China (e-mail: gh.zhang@sub.siat.ac.cn).

C. C. Y. Poon is with the Joint Research Centre for Biomedical Engineering, The Chinese University of Hong Kong, Shatin N.T., Hong Kong (e-mail:cpoon@ee.cuhk.edu.hk).

Y. Li is with the Institute of Biomedical and Health Engineering, Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences, China (e-mail: ye.li@sub.siat.ac.cn).

Y. T. Zhang is with the Joint Research Centre for Biomedical Engineering, Chinese University of Hong Kong, Shatin N.T., Hong Kong, and also with the Key Laboratory of Biomedical Informatics and Health Engineering, Chinese Academy of Sciences, China (e-mail:ytzhang@ee.cuhk.edu.hk).

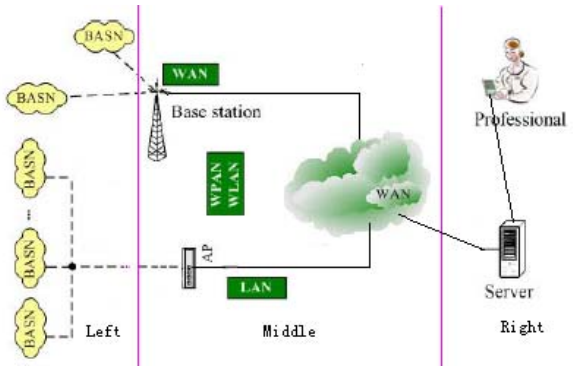

Fig. 1. A telemedicine system architecture [4]

These data must be transmitted to the remote server for telemedicine purpose. Second, all physiological data collected from patients need to be transmitted to the remote server via wired or wireless networks such as the local area network (LAN), wide area network (WAN), wireless person area network (WPAN) or wireless local area network (WLAN) and access point (AP). Third, physicians or professionals who have access to the information can also provide a secured telediagnosis for patients.

Indeed, protecting physiological data for patients is a legal requirement as per the Health Insurance Portability and Accountability Act (HIPAA) [5]. The BSN has its own characteristics [6], [7], which render the traditional security methods of wireless sensor network (WSN) unsuitable: As most biomedical sensors are designed without user-interface, personal identification number (PIN) code of IEEE 802.15.1 is not applicable to BSNs. The public-key mutual authentication between controller and other devices in IEEE802.15.3 would be inappropriate for BSNs because it is computationally expensive. The strategy of using an access control list (ACL) in IEEE 802.15.4 is not applicable to BSNs because of its memory requirement and non-efficient organization. The authors in [7] proposed an approach, wherein biometrics derived from the body were used for securing data transmission in BSN. This method obviated the need for expensive computation and avoided unnecessary communication. Poon *et al*. proposed using inter-pulse intervals (IPI) as the biometric trait for authentication identity or securing the distribution of a cipher key to secure BSN communications [8]. Bao *et al*. suggested that IPI can be used as a biometric characteristic to generate identity of the individual [4]. Though IPI meets all the requirements of a physiological key source mentioned in [8], the authors in [9] presented that it had two principal drawbacks: the value of IPI measured at two different sensors had small differences and using IPI values as keys was slow for the real-time requirements of the BSN.

Bui *et al*. described biometric methods for secure communications in BSN, including a resource-efficient key management system for generating and distributing cryptographic keys and a novel data scrambling method which based on interpolation and random sampling [10]. Challa *et al*. presented an energy efficient key establishment scheme for BSN. The use of biometrics to generate session key eliminated the need of computationally costs of key generation, reduced crosstalk interference between different subjects and avoided possibility of reflection attacks [11].

Up-to-date, security studies for telemedicine applications were few. Some previous studies focused on the BSN security [6]-[8], [10], [11], but the security from BSNs to the remote server and the security between the remote server and physicians in telemedicine systems did not get sufficient attention.

II. TELEMEDICINE SECURITY

A. Intra-BSN security

In the three-step security scheme, the first step is to secure communication within a BSN, which consists of miniaturized, low power and noninvasive or invasive biosensors that are seamlessly placed on or implanted in human body. As shown in Fig. 2, each biosensor of a BSN is capable of processing its own task, encrypting the data and communicating with a Local Processing Unit (LPU) or PDA of the BSN.

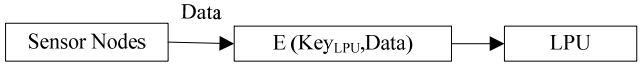

Fig. 2. Data encryption in the BSN

Asymmetric cryptosystems has a much higher computation complexity than symmetric cryptosystems. Therefore it is preferred to use symmetric keys Key_{LPU} to secure the communication between the biosensors and LPU.

B. The BSN to the server security

Securing data communication between a BSN and the remote server is the second step in this security scheme. LPU must send the data to a remote server by WAN, WPAN, WLAN, LAN, etc. The LPU collects these data from sensor nodes and communicates with the remote server. As shown in Fig. 3, all these data should be encrypted by Key_{server} that shares between the LPU and the remote server.

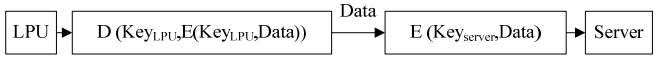

Fig. 3. Data encryption between the LPU to the remote Server

C. Professionals to the server

In this step, both wire and wireless communication networks can be used to promptly and safely transmit the data of a patient in real-time to a practitioner for analysis. The communicating parties (professionals and the remote server) will possess a key that allow them to perform data encryption and decryption by an inexpensive mechanism.

III. KEY GENERATION

We use the following notation to describe key generation in this article:

SN is a sensor node in BSN, and RS is the remote server. PR is a professional or physician in the telemedicine systems.

K_{init} is a predefined initial symmetric key to be modified by the communicating parties.

Key_{LPU} is a symmetric key that shares by SN and LPU.

Key_{server} is a symmetric key that shares between LPU and RS.

Key_{phy} is a symmetric key that shares between PR and RS. DATA denotes patients' data without encryption.

FUN(DATA, k) is a function that returns a k bit random number generated from DATA or a combination of multiple DATA. In section IV, we use PPG as DATA in FUN function and get IPI from it, then we map the results in $[0, 2^k]$. Finally, we can get k bit random number from the results.

MAC(key, DATA, S/R) denotes the computation of the message authentication code (MAC) of DATA with a key such as Key_{init} ,Key_{LPU} by the sender or receiver (S/R).

E(key, DATA) and D(key, DATA) denote the encryption and decryption of DATA respectively.

Key generation is a very important step in cryptosystem and generally consumes a significant amount of computational resource. Key generation consists of three phrases: the initialization, processing and commitment of keys.

A. Key generation in BSN

The idea of using physiological signals for securing biosensor communication was introduced in [6]. IPI, heart rate variability (HRV), ECG can be used in key agreement, entity authentication and BSN security [7]-[9].We can utilize these values to generate the session key for securing data transmission of telemedicine systems. The LPU will set the maximum time to live (TTL) for Key_{LPU}. The details of Key_{LPU} generation are described below:

During Initialization of keys, SN sends E(K_{init} ,DATA) and MAC(E(K_{init} ,DATA, S)) to the LPU.

The Key_{LPU} generation in BSN is depicted in Fig. 4.

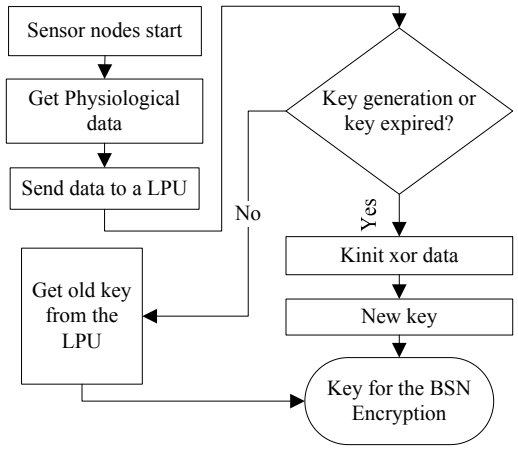

Fig.4. Key generation step in the BSN

In the processing of keys, if SN does not need to generate a new key, then the LPU returns Key_{LPU} directly and go to commitment phase. Otherwise the MAC of encrypted data is computed and verified with MAC from SN. If it matches then it is decrypted with K_{init}:

$DATA = D(K_{init}, E(K_{init}, DATA))$;

$Key_{LPU} = K_{init}$ XOR FUN(DATA, k)

Otherwise it is discarded.

During the commitment of keys, the LPU transmits $E(K_{init}, K_{LPU})$ and $MAC(E(K_{init}, K_{LPU}, S))$ to SN.

After SN receives the data, the MAC of encrypted K_{LPU} is computed and is verified with MAC from LPU, if it does match then it is decrypted with K_{init}:

$K_{init} = D(K_{init}, E(K_{init}, K_{LPU}))$

Otherwise LPU must be informed about this.

SN will transmit $E(K_{init}, DATA)$ and $MAC(E(K_{init}, DATA, S))$ to the LPU, and the MAC of encrypted data is computed and is verified with MAC from SN after the LPU receives the data. If it does match then it is decrypted with K_{LPU} and Key_{LPU} generation is successful:

$K_{init} = Key_{LPU}$

Otherwise Key_{LPU} generation is failed.

B. Key generation between BSNs with the server

The LPU should first decrypt the encrypted data from SN. The LPU will set the maximum time to live (TTL) for Key_{server}. The Key_{server} generation is shown in Fig. 5.

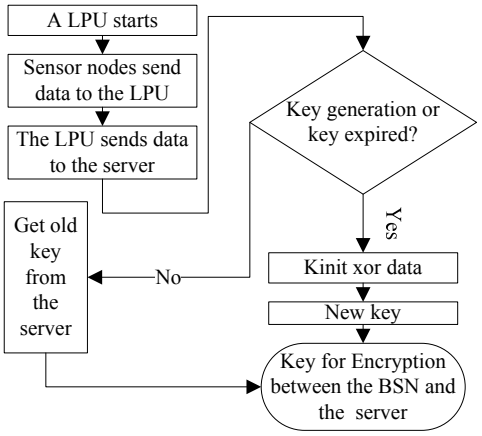

Fig.5. Key generation step between the BSN and the server

C. Key generation between the server and physicians

The server will also set the maximum time to live (TTL) for Key_{phy}. Before professionals send data to the remote server, they must accept identity verification of another party over insecure channels. The initialization and commitment of keys are same as those described in the first step, so we only present the processing of keys in this step:

During the processing of keys, when RS receives message from PR, it will check to make sure the TTL of K_{init} is not expired, and then the MAC of encrypted data is computed and is verified with MAC from PR. If it does match then it is decrypted with K_{init}.

If (K_{init} expired) **Then**

$Key_{phy} = K_{init}$ XOR FUN(DATA, k)

Else

Return Key_{phy} and go to Commitment

End If

Otherwise it is discarded.

Fig. 6 shows the key_{phy} generation between PR and RS.

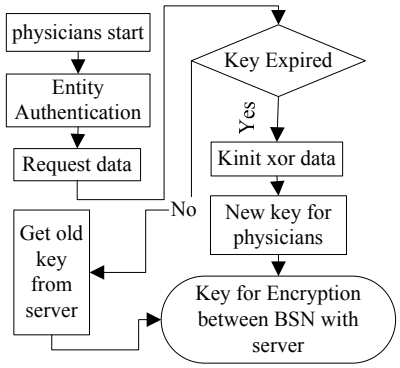

Fig. 6. Key generation between the server and professionals

IV. Performance Analysis

A. Time estimates for brute-force attack

Assume that a brute-force attack is the most efficient attack against an algorithm. Conventional telemedicine systems only have one symmetric key at each communication step. For a key with k bits, there will be 2^k possible combinations of correct key.

In the first step of our security method, if a BSN has n sensor nodes and each sensor node shares a symmetric Key_{LPU} of k bits with LPU and changes t times, then the complexity of a brute-force attack is:

$$F = \sum_{i=1}^{n}\sum_{i=1}^{t} F(i), \mathrm{F(i)} = 2^{\mathrm{k}}. \quad (1)$$

In the second-step, we assume a Key_{server} has m bits and changes s times. The complexity of a brute-force attack is:

$$S = \sum_{i=1}^{s} S(i), \mathrm{S(i)} = 2^{\mathrm{m}}. \quad (2)$$

In the last-step, we assume a Key_{phy} has h bits and changes r times, and then the complexity of a brute-force attack is:

$$\mathrm{L} = \sum_{i=1}^{r} L(i), \mathrm{L(i)} = 2^{\mathrm{h}}. \quad (3)$$

The total complexity is therefore T= F+S+L, and the minimal complexity is: MinC=min(F, S, L). Table I compares the time estimated for attacking a system that use the conventional method and our proposed security method.

TABLE I
THE ATTACKING TIME ESTIMATION OF DIFFERENT LENGTH KEYS

Key length (k,m,h)	Conventional method (second)	Our security method (second)
8	2.6×10^{-10}	2.6×10^{-7}
16	6.5×10^{-8}	6.5×10^{-5}
32	4.3×10^{-3}	4.3

We set k=m=h, n=10, s=100, r=100, t=80 and assume using a machine consisted of a million chips, each capable of testing a million keys per second. Such a machine could test 2^{56} keys in 20 hours.

B. *Randomness of keys*

To test the randomness of the keys generated by the proposed scheme, we generate keys of different lengths from PPG collected at 250 Hz from 12 subjects. Data were collected from each subject for 10 seconds. The IPI were used to generate keys of different bits by our proposed scheme.

Fig. 7 shows that the quantity of keys under the different key length.

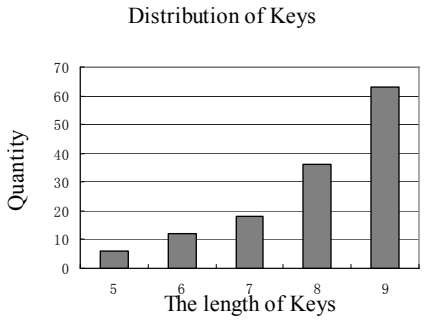

Fig. 7. The distribution of keys quantity (there are 12 subjects, and each subject generate 13 keys by there IPI).

Fig. 8 shows that the probability of different length of keys by using our proposed key generation scheme. The result shows that the probabilities are random enough under the different length of keys.

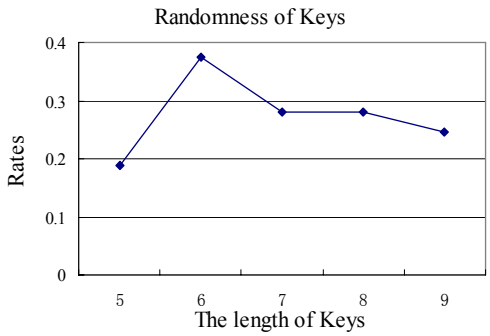

Fig. 8. The randomness of keys generation

V. Discussion and Conclusion

In this paper, we presented a brief analysis of the security provided by our three-step security scheme. Our scheme has a number of advantages, one of which is the generation of key without a pseudo-random generator. We directly use physiological data to generate high-quality, but different, random numbers in each step as the key for securing wireless communication between the sensor nodes and LPU of a BSN, between LPU of different BSNs and the server as well as between the server and different professionals accessing the server.

Using the proposed scheme, physiological signals detected by biomedical sensors have dual functions: for health and medical purposes as well as for securing data transmission. Simulation results show the keys generated by the proposed scheme are more difficult to be estimated as compared to the conventional method. Bao *et al*. verified that some physiological characteristics were random in [12]. Therefore, we can use these physiological characteristics to implement our scheme. In addition, we can implement one-time pad if we generate the key per data transmission.

We assume that physiological data for key generation are already available. If the storage space of physiological data that were needed to generate key is L, then the amount of storage space required is 2L bytes. The space complexity of the key generation can be expressed as O(L). Since the operation of key generation can be performed by bit operations, the time complexity of the key generation can also be expressed as O(L).

Acknowledgment

The authors wish to acknowledge Dr. Z. H. Wang and Dr. X. F. Teng for improving the readability of this paper, Dr. L. Wang for several helpful discussions, and their comments.

References

[1] R. L. Bashshur, T.G. Reardon, and G. W. Shannon, "Telemedicine: A New Health Care Delivery System," Ann. Rev. Public Health, vol. 21, 2000, pp. 613-17.

[2] T. L. Huston and J. L. Huston, "Is Telemedicine a Practical Reality?" Commun. ACM, 43, 6 (June 2001), 91-95.

[3] http://www.wisegeek.com/what-is-telemedicine.htm

[4] S. D. Bao, Y. T. Zhang, and L. F. Shen, "Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems", in Proc. 27th Annual Conf. IEEE-EMBS, Shanghai, China, Sep.2005.

[5] HIPPA-Report 2003, "Summary of HIPPA Health Insurance Probability and Accountability Act," US Department of Health and Human Service, May 2003.

[6] S. D. Bao, Y. T. Zhang and L. F. Shen, "A design proposal of security architecture for medica1 body sensor networks", in Proc. of International Workshop on Wearable and Implantable Body Sensor Networks: 84—90, MIT, Cambridge, USA. 3-5 April. 2006.

[7] S.Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body," Proc. IEEE int'l. Conf. Parallel Processing Wksp. 6-9, pp. 432-39, Oct. 2003.

[8] C. C. Y. Poon, S. D. Bao, and Y. T. Zhang, "A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-health", to appear in IEEE Communications Magazine, Apr. 2006.

[9] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "EKG-based Key Agreement in Body Sensor Networks", in Computer Communications Workshops, 2008, INFOCOM, IEEE Conference, pp. 1-6, April 2008.

[10] F. M. Bui and D. Hatzinakos, "Biometric Methods for Secure Communications in Body Sensor Networks: Resource-Efficient Key Management and Signal-Level Data Scrambling",in Eurasip Journal on Advances in Signal Processing, Volume 2008.

[11] N. Challa, H. Cam, and M. Sikri, "Secure and Efficient Data Transmission over Body Sensor and Wireless Networks", in Eurasip Journal on Advances in Signal Processing, Volume 2008.

[12] S. D. Bao, L. F. Shen, and Y. T. Zhang, "A Novel Key Distribution of Body Area Networks for Telemedicine", in Proc. IEEE Int. Workshop on Biomedical Circuits and Systems, Singapore, Dec. 2004,pp.S2.1-17-20.