

A Secure Medical Information Management System for Wireless Body Area Networks

Xiyao Liu¹, Yuesheng Zhu², Yu Ge³, Dajun Wu³ and Beiji Zou¹

1. School of Information Science and Engineering, Central South University, Changsha, Hunan Province, P.R. China, 410083

[lxyzoewx@csu.edu.cn; bjzou@csu.edu.cn]

2. The Communication and Information Security Lab, Institute of Big Data Technologies, Shenzhen Graduate School, Peking University, China

[zhuys@pkusz.edu.cn]

3. Institute for Infocomm Research, Singapore

[geyu@i2r.a-star.edu.sg; djwu@i2r.a-star.edu.sg]

*Corresponding author: Yuesheng Zhu²

*Received June 4, 2015; revised September 24, 2015; accepted November 8, 2015;
published January 31, 2016*

Abstract

The wireless body area networks (WBANs) consist of wearable computing devices and can support various healthcare-related applications. There exist two crucial issues when WBANs are utilized for healthcare applications. One is the protection of the sensitive biometric data transmitted over the insecure wireless channels. The other is the design of effective medical management mechanisms. In this paper, a secure medical information management system is proposed and implemented on a TinyOS-based WBAN test bed to simultaneously address these two issues. In this system, the electronic medical record (EMR) is bound to the biometric data with a novel fragile zero-watermarking scheme based on the modified visual secret sharing (MVSS). In this manner, the EMR can be utilized not only for medical management but also for data integrity checking. Additionally, both the biometric data and the EMR are encrypted, and the EMR is further protected by the MVSS. Our analysis and experimental results demonstrate that the proposed system not only protects the confidentiality of both the biometric data and the EMR but also offers reliable patient information authentication, explicit healthcare operation verification and undeniable doctor liability identification for WBANs.

Keywords: Wireless body area network, electronic medical record, secure medical information management, fragile zero-watermark, visual secret sharing.

1. Introduction

Wireless body area networks (WBANs) consist of small wearable or implantable sensors on, near, or in a human body. By collecting vital sign parameters and activities from a human body, WBANs can enable continuous health monitoring and provide portable, real-time and ubiquitous healthcare services, and offer numerous practical and innovative applications to improve healthcare quality [1-9]. The security of WBANs is critical for those healthcare applications because the sensitive biometric data have to be exchanged over insecure networks. Moreover, medical management is an important issue for all the healthcare applications. Therefore, the design of effective medical management mechanisms for WBANs is also indispensable.

The primary security threats to a healthcare system over WBANs include eavesdropping, data modification and impersonation attack [10-11]. Some secure protection methods, such as encryptions, integrity authentications [12-13], sensor node authentications [14-18] and secure key managements [19-23] have been developed to defend against these threats. Those approaches can partially deal with those security threats over WBANs, but few of them draws attention to the medical management issue and includes effective medical management mechanisms with secure protections simultaneously. As mentioned in the preceding paragraph, it is better to simultaneously address the security and the medical management issues in WBANs for healthcare applications. Therefore, there is still plenty of room for improvement.

In medical management, patient information authentication, healthcare operation verification and doctor liability identification are the important areas in need of research. The applications of WBANs can draw lessons from the existing approaches [24-27] for medical image applications, in which the electronic medical record (EMR) containing prime healthcare information is directly embedded into a medical image by watermarking schemes for patient authentication and data integrity check. However, the watermarking schemes cannot be directly applied to the healthcare applications over the WBANs for two reasons. Firstly, most of those schemes [24, 26-27] will unavoidably modify the watermark carriers in order to embed the EMR. However, as the watermark carriers in WBANs are sensitive biometric data and must not be modified, the lossless watermarking scheme has to be used for WBANs. Secondly, because the sizes of typical biometric data are much smaller than those of medical images, the watermark embedding capacity would be insufficient for hiding the EMR.

Recently, zero-watermarking algorithms [28-30] have attracted much attention. Rather than directly embedding information into watermark carriers as traditional watermarking algorithms do, a master share and an ownership share are generated according to the visual secret sharing [31] (VSS) to bind the information with the watermark carriers in those methods. Although those methods were originally designed for copyright protection applications, they have the potential to be applied in WBANs due to the following four advantages. Firstly, the watermark carriers are not modified for hiding the watermark. Secondly, there is no limitation of watermark embedding capacity. Thirdly, the computational cost of shares generation according to the VSS is low. Lastly, the utilization of the VSS can further enhance the protection of data confidentiality since the VSS is similar to a method of encryption.

In this paper, we propose a secure medical information management system (SMIMS) for WBANs. The key points of our work are as follows:

- 1) The system is innovatively designed, to simultaneously address the issues of security and medical management for WBANs, and the EMR is utilized to authenticate the patient information, verify the healthcare operation and identify the doctor liability.
- 2) A novel fragile zero-watermarking scheme based on the modified visual secret sharing (MVSS) is proposed, in which the EMR is used as the watermark information and strictly bound to the biometric data. In this manner, the medical management based on the EMR is reliable and undeniable and the EMR can be utilized to check the authenticity and integrity of biometric data because the proposed zero-watermarking scheme is fragile.
- 3) The benefits of the robust zero-watermarking schemes are inherited by the proposed fragile zero-watermarking scheme. Therefore, the proposed scheme is suitable for WBANs.
- 4) The confidentiality of both the biometric data and its bound EMR are well protected in our proposed SMIMS
- 5) The proposed SMIMS is implemented on a TinyOS-based WBAN test bed rather than merely emulated on a PC.

The rest of the paper is organized as follows. In Section 2, our proposed SMIMS for WBANs is described in detail. The performance of the proposed SMIMS is analyzed in Section 3, and the experiment results are shown in Section 4. Finally the conclusions of the paper are given in Section 5.

2. Proposed Secure Medical Information Management System (SMIMS) for WBANs

The architecture of the SMIMS is shown in [Fig. 1](#).

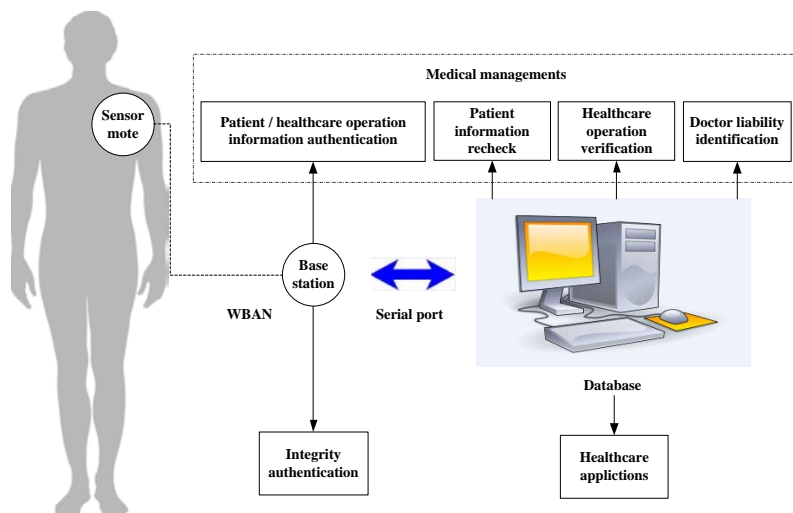


Fig. 1. The architecture of the SMIMS.

The biometric information is collected by the on-body sensor mote and transmitted securely with the EMR to the base station over WBANs. The patient information, the healthcare operation information and the integrity of biometric data are authenticated at the base station, which is connected to databases for medical managements and further healthcare applications. If they are all correctly authenticated, the crucial data are stored in databases. The assumptions and the details of the SMIMS are illustrated as follows.

2.1 The assumptions of the SMIMS.

In this paper, the following assumptions are made:







- 1) The deployment of sensors with the pre-stored information to the patient is secure. There is no error of pre-stored information.
- 2) We are primarily concerned with the three threats resulting from the wireless channel, which are data eavesdropping, data modification and impersonation attack.
- 3) The symmetric keys have been previously distributed, and we mainly focus on the processes after the key management and establishment.
- 4) As another reference for security in WBANs [17], there is a secure storage in the sensor mote and the critical information stored in the storage will not leak even if it is physically captured by an unauthorized person.

2.2 Modified VSS

In this section, the concepts of the VSS and modified VSS are illustrated to facilitate the description of the system procedures in Section 2.3.

The (m, n) VSS (where $m \leq n$) was proposed by Naor and Shamir [31]. In this scheme, a binary image is split into n shares, and can be reconstructed from l shares when $l \geq m$, otherwise the image cannot be reconstructed. The $(2, 2)$ VSS is a typical VSS, in which a white pixel is split into two identical shares whereas a black pixel into two complementary shares as shown in Table 1. The white pixel represents the bit '1', and the black pixel represents the bit '0'.

Table 1. Original $(2, 2)$ VSS







Pixel value	1(white pixel)	0(black pixel)
Master share		
Ownership share		
Stack result		

The pixel expansion will occur during the share splitting process in the original $(2, 2)$ VSS [31], *i.e.*, the size of the shared information is 2×2 times larger than the original information. Take a bit '1' for example, its shared information should be 4 bits vectors such as '0,1,1,0' or '1,0,0,1' when the VSS is utilized in WBANs. Considering the limited bandwidth in WBANs, the pixel expansion is unacceptable.

To solve this problem, Surekha [29] proposed the modified $(2, 2)$ VSS scheme (MVSS), in which the share splitting and stacking process are designed based on the EXCLUSIVE-OR function as shown in Table 2. In this manner, no pixel expansion will occur, and thus the

sizes of the shared and the original information are exactly the same. The MVSS is more suitable for WBANs because of the limited bandwidth.

Table 2. Modified (2, 2) VSS

Pixel value	1(white pixel)	0(black pixel)
Master share		
Ownership share		
Stack result		

Utilizing the MVSS can solve the problem of pixel expansion, but the shared information generated from the identical original information would be identical and does not hide information patterns well. Essentially, it does not provide strict data confidentiality. To overcome this drawback, we draw lessons from the Counter Mode of Advanced Encryption Standard (AES-CTR) and propose a novel fragile zero-watermarking scheme based on the MVSS with AES-CTR. With this method, the EMR is bound to the biometric data and their confidentiality are enhanced.

2.3 The procedures of the SMIMS

The SMIMS consists of three phases: the Pre-deploy phase, the EMR sharing phase, and the EMR identification phase. Firstly, The EMR is stored in the secure storages of the on-body sensor and base station in the Pre-deploy phase. Then, the ownership share of the EMR is generated, and the original biometric information is encrypted in the EMR sharing phase. Both of them are transmitted to base station as payloads of packets. Finally, the original biometric information is decrypted and the EMR is recovered in the EMR identification phase. The detailed procedures are described as follows.

2.3.1 Pre-deploy phase:

The Pre-deploy phase is executed before the EMR sharing and the EMR identification phase, in which the m bytes EMR W is pre-stored into the secure storages of the sensor mote and base station. The EMR cannot be changed in any subsequent phases after it is pre-bound to sensor mote and base station.

2.3.2 EMR sharing phase:

After the Pre-deploy phase is finished, the EMR sharing phase is executed. The block diagram of the EMR sharing phase is shown as **Fig. 2**, and its detailed steps are illustrated below:

- 1) Encrypt the original biometric information P into the cipher text S utilizing the AES-CTR encryption as shown in equ.1

$$\begin{aligned} L &= E(k, C); \\ S &= L \oplus P \end{aligned} \quad (1)$$

where k is the symmetric keys which have been previously distributed, $E(.)$ is the encryption of the Electronic Codebook Mode of Advanced Encryption Standard (AES-

ECB), C is constructed with the 15 bytes nonce and the 1 byte counter, and L is the cipher text of C . Once the lengths of P and L are different, perform EXCLUSIVE-OR operation iteratively.

- 2) Perform the SHA-1 function on the original biometric information P and get the 20 bytes hashed vector V .

$$V = SHA-1(k \parallel P) \quad (2)$$

where $SHA-1(.)$ is the SHA-1 function and \parallel is the concatenation operator.

- 3) Split the 20 bytes vector V into two 10 bytes vectors. Then, combine the two 10 bytes vectors with the last 5 bytes of the nonce and the 1 byte counter used in the AES-CTR process to form two new 16 bytes data. Finally, melt them into a 32 bytes data F .

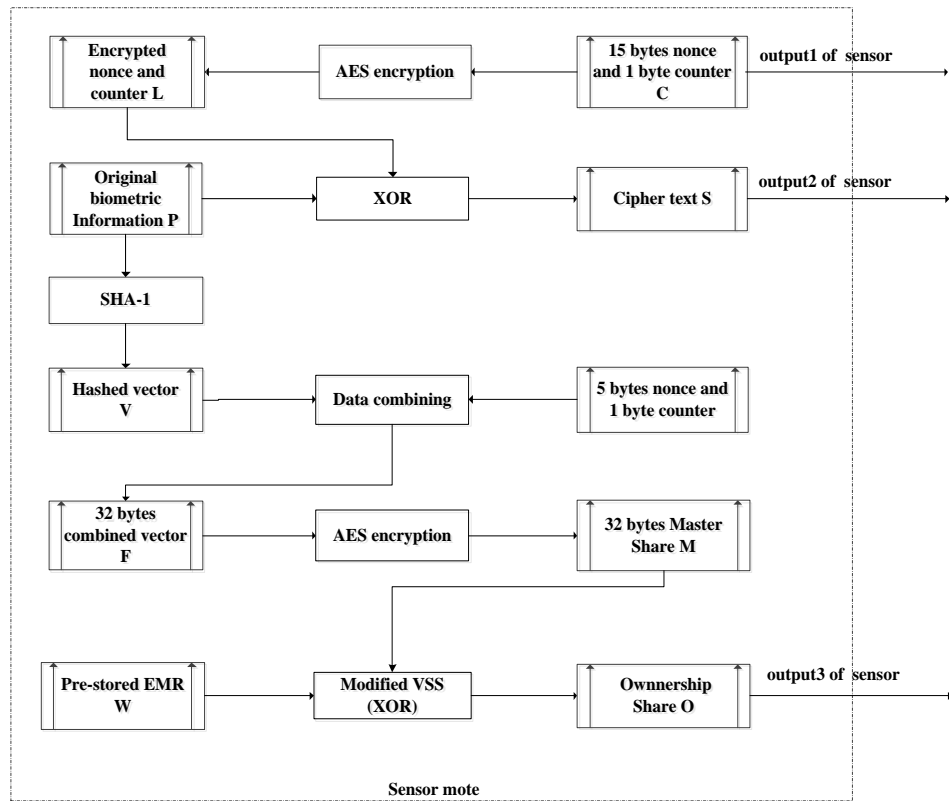


Fig. 2. The block diagram of the EMR sharing phase.

- 4) Perform the AES-ECB encryption on F to generate a 32 bytes master share M . The master shares M generated with identical biometric information will be different thereby enhancing the data confidentiality.

$$M = E(k, F) \quad (3)$$

- 5) Construct an ownership share O from M and the EMR W according to the modified VSS. Once the lengths of M and W are different, perform the EXCLUSIVE-OR operation iteratively.

$$O = M \oplus W \quad (4)$$

- 6) Transmit the packet including the 15 bytes nonce, the 1 byte counter, the encrypted original biometric information S , and the generated ownership share O to the base station.

2.3.3 EMR identification phase:

After the transmitted packet is received, the EMR identification phase is executed. The block diagram of the EMR identification phase is shown as Fig. 3, and its detailed steps are described below:

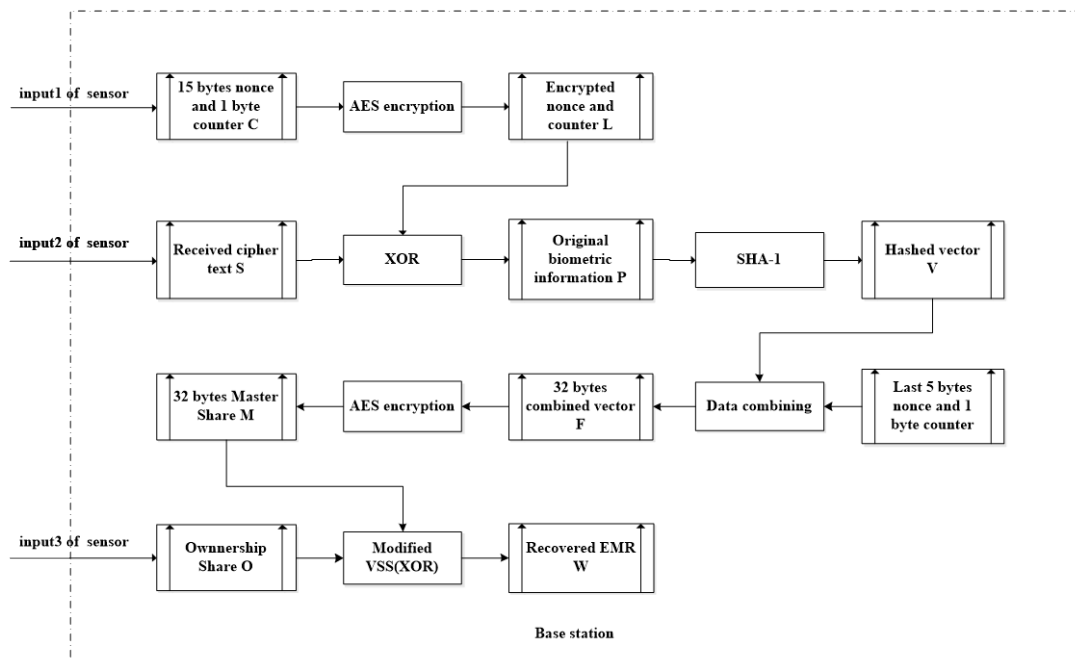


Fig. 3. The block diagram of the EMR identification phase.

- 1) Decrypt the encrypted information S to recover the original biometric information P as shown in Eq.(5).

$$\begin{aligned} L &= E(k, C); \\ P &= L \oplus S \end{aligned} \quad (5)$$

where k is the symmetric keys which have been previously distributed, $E(\cdot)$ is the AES-ECB encryption, C is the received 15 bytes of the nonce and the 1 byte counter and L is the cipher text of C .

- 2) Perform the SHA-1 function on the original biometric information and get the hashed vector V .
- 3) Split the binary vector V into two 10 bytes vectors and combine them with the last 5 bytes of nonce and the 1 byte counter to form a 32 bytes data F .

- 4) Perform the AES-ECB encryption on F to generate the 32 bytes master share M .
- 5) Recover the EMR W from the master share M and its relevant ownership-share O , according to the modified VSS. Once the lengths of M and O are different, perform EXCLUSIVE-OR operation iteratively.

$$W = M \oplus O \quad (6)$$

- 6) Compare the recovered EMR with the pre-stored one to check the integrity of biometric information and the authenticities of patient and healthcare operation information.
- 7) If the patient information, the healthcare operation information and the integrity of biometric data are all correctly authenticated, the biometric information P is stored into a medical information database for further medical applications. Additionally, its relevant ownership-share O , the last 5 bytes of the nonce and the 1 byte counter are also needed to be stored in a medical management database to enable the recovery of the EMR for patient information rechecking, healthcare operation verification and doctor liability identification.
- 8) The access of the medical management database is denied unless the recovery of EMR is needed.

3. System Analysis

The performances of the security function, medical management function and system practicability are analyzed as follows.

3.1 Analysis of security function

Table 3. The protection mechanisms for different types of attacks

The type of attack	The protection mechanism
Eavesdropping	MVSS, AES-CTR encryption
Modification	MVSS, AES-CTR encryption, EMR authentication
Impersonation attack	MVSS, AES-CTR encryption, EMR authentication

The protection mechanisms of the SMIMS against different types of attacks are summarized in **Table 3**, and the details of analyses for each type of attack are illustrated below.

3.1.1 Threats of Eavesdropping

1) Biometric data

The biometric data are protected by AES-CTR encryption. Therefore, no one can obtain the genuine plaintext without the correct key.

2) EMR

Due to the utilization of the MVSS, the mere plaintext of ownership share does not contain any EMR, and the EMR can be eavesdropped only if the attackers obtain both the ownership share and its relevant master share. In addition, the master share can only be

obtained by the hash of biometric data which is well protected by the AES-CTR encryption. Therefore, the confidentiality of the EMR is guaranteed.

3.1.2 Threats of data modification

1) Biometric data

The hash value V of the biometric data will be completely different even if the biometric data are merely changed by one bit. Therefore, the master shares M generated by encrypting V will also be completely different, leading to a completely different recovered EMR.

2) Ownership share

If the ownership share is modified, the EMR recovered according to the MVSS will be different from the pre-stored one.

3) Nonce and counter

If either the nonce or the counter is modified, the decryption of the biometric data will fail, and the hash value V of the decrypted biometric data will be completely wrong and thus the EMR recovered by the MVSS will be different from the pre-stored one.

As summarized in Table 4, due to the utilization of the fragile zero-watermarking based on the MVSS with AES-CTR encryption, any modification will lead to a wrongly recovered EMR and thus the data modification can be reliably inspected by the EMR authentication.

Table 4. The effects of data modifications

Type of attack	Decrypted biometric data	Ownership share	Recovered EMR	EMR authentication
Modify the cipher text of the biometric data	Wrong	Not changed	Wrong	Fail
Modify the ownership share	Correct	Changed	Wrong	Fail
Modify the nonce and counter	Wrong	Not changed	Wrong	Fail

3.1.3 Threats of impersonation attack

It is hard to forge the EMR because it is pre-stored in a secure environment and protected by the AES-CTR encryption and MVSS during the transmission. The rate of a successful impersonation of the correct EMR is merely $(1/256)^m$, of which the value is extremely small when the m is large, where m is the length of the EMR. Therefore, the threats of impersonation attack can be prevented by comparing the recovered EMR with the pre-stored one.

3.2 Analysis of medical management function

To satisfy the requirement of medical management, the EMR can be recovered by using the biometric data and the relevant ownership share stored in the databases. Because the EMR is pre-stored inside the sensors in Pre-deploy phase and no one can modify this information subsequently, the patient and healthcare operation information can be authenticated or rechecked reliably by the EMR. Additionally, since the EMR is strictly bound to the hash value of biometric data and the probability of hash collision is close to zero, the identification of doctor liability based on the EMR is undeniable.

3.3 Analysis of practicability:

1) High-efficiency

The computational complexity of the SMIMS is analyzed to demonstrate its efficiency.

For the Pre-deploy phase, its computational complexity is insignificant compared with the other two phases because the phase is executed once while the other two phases are executed many times in one healthcare operation.

For the EMR sharing phase, one sharing procedure includes the generation of a random number, a SHA-1 function for the biometric data P , an AES encryption of the 15 bytes nonce with the 1 byte counter, an AES encryption of the 32 bytes combined vector F and a calculation of the MVSS. The computational complexity of the MVSS function (EXCLUSIVE-OR operations) is insignificant and thus the computational complexities of other functions are mainly discussed here. It is assumed that the length of biometric data is l bytes without loss of generality. Firstly, in order to calculate the SHA-1 value, the biometric data are divided into $\lceil l \times 8 / 512 \rceil$ blocks and each block is iterated for 80 rounds, where $\lceil \cdot \rceil$ is the top integral function. In each round, 66 SHIFT operations, 272 EXCLUSIVE-OR operations, 20 NOT operations, 100 bitwise AND operations and 60 bitwise OR operations are executed. All of those operations are simple and do not lead to a high computational complexity. Secondly, it requires 160 MULTIPLY-ADD operations and 120 EXCLUSIVE-OR operations for encrypting each 16 bytes of data. In addition, all the AES encryptions are implemented based on hardware to further reduce their computational complexity. Finally, it calls the built-in library functions of nesC for the generation of random numbers. Based on the above analyses, the computational complexity of one sharing procedure is demonstrated to be low.

For the EMR identification phase, one identification procedure includes a SHA-1 function for the biometric data P , an AES encryption of the 15 bytes nonce with the 1 byte counter, an AES encryption of the 32 bytes combined vector F , a calculation of the MVSS and the authentication of EMR, which is similar to one sharing procedure. Therefore, the computational complexity of one identification procedure is also low.

2) User-friendliness

Because the recovered EMR contains the prime information of the healthcare operation, such as the personal information of patients, the healthcare operation ID and the doctor ID, the patient information authentication, the healthcare operation verification and the doctor liability identification can be executed conveniently and concisely. It indicates that our proposed system is user-friendly.

3) Convenience

In the SMIMS, our modules are implemented in the on-body sensors and the medical databases, without incurring any additional hardware cost.

4. Experiment Results

4.1 Establishment of experiments

The proposed scheme is implemented on a WBAN test bed based on TinyOS 2.x using nesC programming language. A MicaZ sensor node, developed by Crossbow Technology [32], is adopted as the sensor mote on an adult body. The sensor node consists of an ATmega128L microcontroller, a 2.4 GHz CC2420 RF transceiver, a 4KB Random-Access Memory (RAM) and a 128KB Read-Only Memory (ROM). A gateway node receives the data from the sensor mote and is connected to a PC for data visualization and analysis. The on-body sensor

executes the EMR sharing phase while the EMR identification phase is carried out on the gateway node. The sensor developed by Sparkfun [33] is utilized to gain real pulse data in our experiments. An EMR, with a length of 32 bytes, is designed for testing as shown in Fig. 4. The EMR includes 4 bytes of patient ID, 1 byte of patient information, 4 bytes of doctor ID, 3 bytes of health operation ID and 20 bytes of note for healthcare operation.

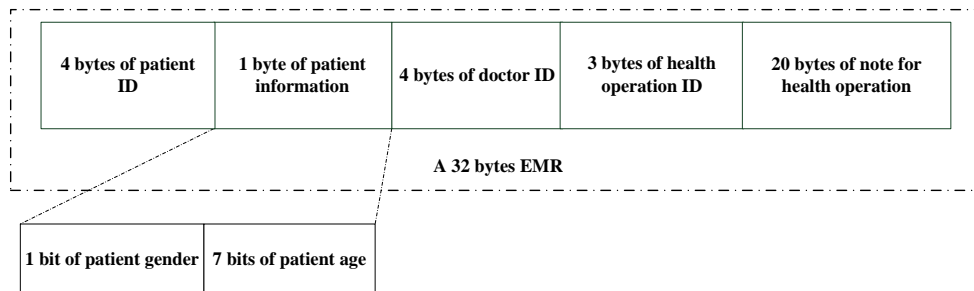


Fig. 4. The EMR designed for testing

The 4 bytes of patient and doctor ID can represent 2^{32} , *i.e.*, more than 4 billion different patients and doctors, and the 3 bytes of healthcare operation ID can represent 2^{24} , *i.e.*, more than 16 million different types of health operations, which are sufficient for the requirements of a majority healthcare applications. The 1 byte of patient information is constructed by 1 bit of patient gender information and 7 bits of patient age information which can represent the patients aged from 0 to 127. The designed EMR contains the prime information to authenticate the patient information, to verify the healthcare operation and identify the doctor liability concisely. In addition, the length of the EMR can be extended and the structure of the EMR can also be transformed according to different requirements of healthcare applications.

In the following sections, the performances of the SMIMS are tested, including the security issue, memory consumption and computation cost.

4.2 Test of security issue

In this section, the security performance of the SMIMS is tested. Firstly, the effectiveness of data confidentiality protection is evaluated, and the relevant data are represented in hexadecimal in **Table 5**.

Table 5. The effectiveness of data confidentiality protection

Counter	Plaintext of biometric data	Cipher text of biometric data	EMR	Ownership share
1	029F02BD	7F605C36	0000000167000000	3D2407D35AC4C642
	02F70345	E5282D3E	0E00000A00000000	0D43032FEE243C28
	038E03B1	16139E5FF	0000000000000000	9FE90F77AF1C010B
	03A50371	C6AD749	0000000000000000	62C57F69F309AD80
2	029F02BD	07D6B4A1	0000000167000000	56F7C617B37B7F15
	02F70345	082DE3F4	0E00000A00000000	F50BF0D32B0B2B2D
	038E03B1	28CD7D8B	0000000000000000	BB2AE50AD228EE74
	03A50371	885A3FE7	0000000000000000	DC0400FC01F0A3A3

Table 5 shows that the cipher texts of biometric data are completely different from their plaintexts and the identical biometric data are encrypted into different ciphers due to applying of AES-CTR encryption. In addition, by utilizing AES-CTR encryption and the MVSS, the mere ownership shares contain no information about the EMR and are

completely different even when they are generated from the identical biometric information with the identical EMR. Therefore, the confidentialities of the biometric data and EMR are significantly protected in the SMIMS.

Then, 4 types of different attacks are performed in the WBANs, including randomly modifying one bit of biometric data, ownership share, nonce or counter and randomly forge an EMR. For each type of attack, the EMRs of 1000 attacked samples are authenticated and all of these fail.

The results are consistent with our analysis given in Section 3.1 and indicate that the threats of data modification and impersonation attack can be detected and prevented in the SMIMS.

4.3 Test of memory consumption

In this section, the memory consumptions of SMIMS are examined and compared with those of the system without security or medical management function whilst the lengths of biometric data are set to different values. The results are shown in Figs 5-6.

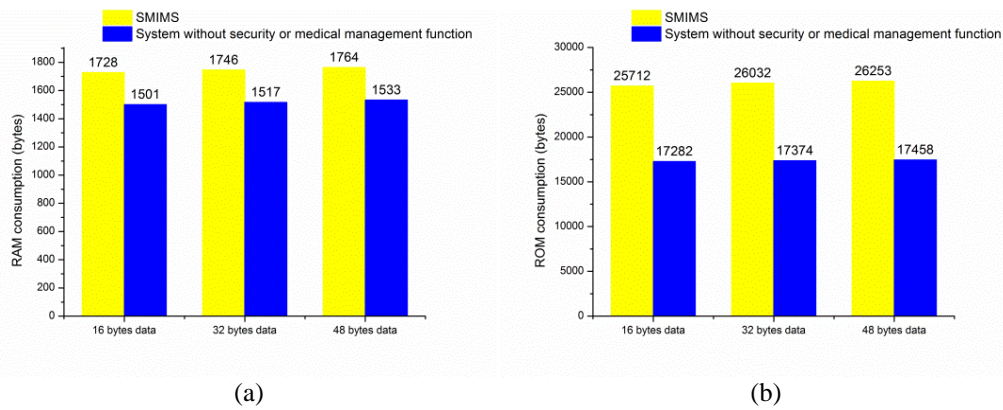


Fig. 5. Memory consumption on the sensor mote: a) RAM consumption, b) ROM consumption

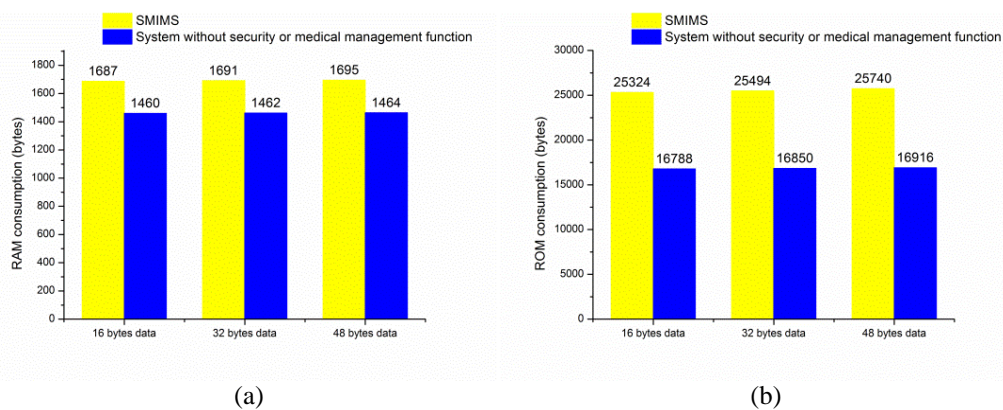


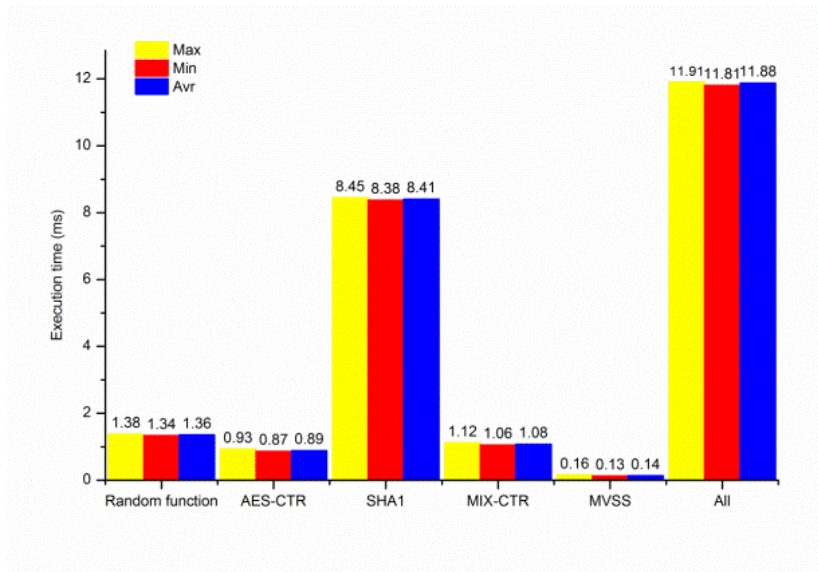
Fig. 6. Memory consumption on the base station: a) RAM consumption, b) ROM consumption

It can be observed from Figs 5-6 that the RAM consumption rates of our SMIMS are less than 50%, which is 2048 bytes, and the ROM consuming rates are even lower. Moreover, Figs 5-6 show that the memory consumptions remain almost unchanged when the length of biometric data increases. Additionally, these two figures demonstrate that the differences between the memory consumptions of the SMIMS and those of the system without any

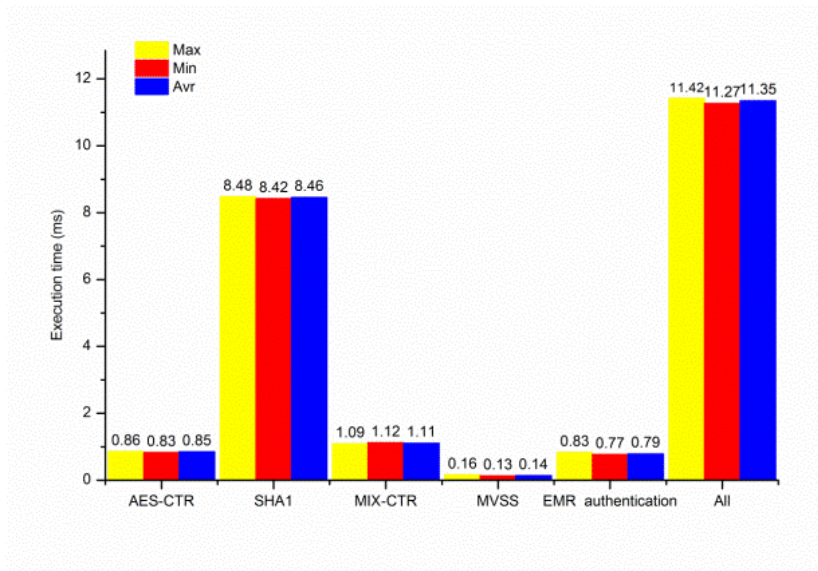
security or medical management function are very small, at less than 250 bytes in RAM and 9000 bytes in ROM.

It is demonstrated that the memory consumptions of all the security and medical management processes are quite low and that the memory consumption of the whole SMIMS is acceptable based on the above results.

4.4 Test of computation cost



(a)



(b)

Fig. 7. Execution time: a) EMR sharing processes, b) EMR identification processes

The computation cost of the SMIMS includes 3 parts: the execution time of the EMR pre-writing, the EMR sharing and the EMR identification processes.

In this section, the execution time of the EMR pre-writing is tested first, and requires only 9.568 ms. Additionally, the pre-writing of the EMR is needed only once for one healthcare operation, its execution time is negligible compared to those of EMR sharing and identification processes since they are executed many times in one healthcare operation.

Then, the execution times of the EMR sharing and identification processes are examined in detail by testing 1000 packets. The results are shown in **Fig. 7**, in which the AES-CTR indicates the encryption function of the 15 bytes nonce with the 1 byte counter and the MIX-CTR indicates the encryption function of the 32 bytes combined vector F .

Fig. 7 shows that the SHA-1 function requires the longest execution time at approximately 9 ms. Moreover, the EMR sharing process has a maximum execution time of 11.91 ms and an average time of 11.88 ms, and the EMR identification process has a maximum time of 11.42 ms and an average time of 11.35 ms. All of these are negligible, which is consistent with our analysis given in Section 3.3 and indicates that the proposed SMIMS is of high-efficiency.

Section 4.4 and 4.5 illustrate that the SMIMS is suitable for WBANs in terms of memory consumption and computation cost.

5. Conclusions

In this paper, a secure medical information management system for WBANs is proposed and implemented on a TinyOS-based test bed to simultaneously address the issues of security and medical management. Our analysis and experimental results have demonstrated that the proposed SMIMS possesses the following merits: the patient and healthcare operation information can be authenticated reliably and explicitly; the doctor liability can be identified without repudiation; the data modification or impersonation attack can be explicitly identified according to the recovered EMR; the data confidentiality is well protected by using the AES-CTR encryption and the MVSS; and both the memory consumption and computation cost of the proposed system are low, indicating that the SMIMS is suitable for WBANs with strict resource constraints.

Acknowledgements

This research is supported by the National Nature Science Foundations of China (61173122, 61573380). The authors would like to thank for the supports from postdoctoral research station of Central South University and the valuable comments on this paper from Mr. Songtao Wu, Dr. Xiaoyu Li and Dr. Rongchang Zhao.

References

- [1] B. Latré, B. Braem, I. Moerman, C. Blondia and P. Demeester, "A survey on wireless body area networks," *Wireless Networks*, vol. 17, no. 1, pp. 1-18, January, 2011. [Article \(CrossRef Link\)](#).
- [2] H. Cao, V. Leung, C. Chow and H. Chan, "Enabling technologies for wireless body area networks: A survey and outlook," *IEEE Communications Magazine*, vol. 47, no. 12, pp. 84-93, December, 2009. [Article \(CrossRef Link\)](#).

- [3] C. Otto, A. Milenkovic, C. Sanders and E. Jovanov, "System architecture of a wireless body area sensor network for ubiquitous health monitoring," *Journal of Mobile Multimedia*, vol. 1, no. 4, pp. 307-326, January, 2006. [Article \(CrossRef Link\)](#).
- [4] M. A. Hanson, H. C. Powell Jr, A. T. Barth, K. Ringgenberg, B. H. Calhoun, J. H. Aylor and J. Lach, "Body area sensor networks: Challenges and opportunities," *Computer*, vol. 42, no. 1, pp. 58-65, January, 2009. [Article \(CrossRef Link\)](#).
- [5] J. Y. Khan, M. R. Yuce, G. Bulger and B. Harding, "Wireless body area network (WBAN) design techniques and performance evaluation," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1441-1457, October, 2012. [Article \(CrossRef Link\)](#).
- [6] S. Lim and H. Lee, "Factors affecting medical incident care on WBAN," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 7, no. 5, pp. 1058-1076, May, 2013. [Article \(CrossRef Link\)](#).
- [7] Y. O. Mohammed and U. A. Baroudi, "Partially observable Markov decision processes (POMDPs) and wireless body area networks (WBAN)," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 7, no. 5, pp. 1036-1057, May, 2013. [Article \(CrossRef Link\)](#).
- [8] T. Hayajneh, G. Almashaqbeh, S. Ullah and A.V. Vasilakos, "A survey of wireless technologies coexistence in WBAN: analysis and open research issues," *Wireless Networks*, vol. 20 no. 8, pp. 2165-2199, May, 2014. [Article \(CrossRef Link\)](#).
- [9] J. Liu, Q. Wang, J. Wan, J. Xiong and B. Zeng, "Towards key issues of disaster aid based on wireless body area networks," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 7, no. 5, pp. 1014-1035, May, 2013. [Article \(CrossRef Link\)](#).
- [10] M. A. Ameen, J. Liu and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of medical systems*, vol. 36, no. 1, pp. 93-101, February, 2012. [Article \(CrossRef Link\)](#).
- [11] M. Li, W. Lou and K. Ren, "Data security and privacy in wireless body area networks," *Wireless Communications, IEEE*, vol. 17, no. 1, pp. 51-58, February, 2010. [Article \(CrossRef Link\)](#).
- [12] C. C. Tan, H. Wang, S. Zhong and L. Qun, "Body sensor network security: an identity-based cryptography approach," in *Proc. of the 1st Conf. on Wireless network security*, ACM, pp. 148-153, March 31–April 2, 2008. [Article \(CrossRef Link\)](#).
- [13] X. Liu, Y. Ge, Y. Zhu and D. Wu, "A Lightweight Integrity Authentication Scheme based on Reversible Watermark for Wireless Body Area Networks," *KSII Transactions on Internet and Information Systems (TIIS)*, vol.8, no.12, pp. 4643-4660, December, 2014. [Article \(CrossRef Link\)](#).
- [14] C.C.Y. Poon, Y.T. Zhang and S.D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 73-81, April, 2006. [Article \(CrossRef Link\)](#).
- [15] K. Zeng, K. Govindan and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 56 – 62, October, 2010. [Article \(CrossRef Link\)](#).
- [16] L. Shi, M. Li, S. Yu and J. Yuan, "BANA: body area network authentication exploiting channel characteristics," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1803-1816, September, 2013. [Article \(CrossRef Link\)](#).
- [17] L. Ma, Y. Ge and Y. Zhu, "TinyZKP: a lightweight authentication scheme based on zero-knowledge proof for wireless body area networks," *Wireless Personal Communications*, vol. 77, no. 2, pp. 1077–1090, July, 2014. [Article \(CrossRef Link\)](#).
- [18] M. Li, S. Yu, J.D. Guttman, W. Lou and K. Ren, "Secure ad hoc trust initialization and key management in wireless body area networks," *ACM Transactions on Sensor Networks*, vol. 9, no. 2, pp. 18-52, March, 2013. [Article \(CrossRef Link\)](#).
- [19] S. Mathur, W. Trappe, N. Mandayam, C. Ye and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proc. of the 14th Int. Conf. on Mobile computing and networking*, ACM, pp. 128-139, September 14–19, 2008. [Article \(CrossRef Link\)](#).
- [20] S. Jana, S.N. Premnath, M. Clark, S.K. Kasera, N.Patwari and S.V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in

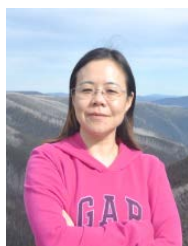
- Proc. of the 15th annual Int. Conf. on Mobile computing and networking, ACM*, pp. 321-332, September 20–25, 2009. [Article \(CrossRef Link\)](#).
- [21] K.K. Venkatasubramanian, A. Banerjee and S.K.S. Gupta, “PSKA: usable and secure key agreement scheme for body area networks,” *IEEE Transactions on Information Technology in Biomedicine*, vol. 14, no. 1, pp. 60-68, January, 2010. [Article \(CrossRef Link\)](#).
- [22] K.K. Venkatasubramanian and S.K.S. Gupta, “Physiological value-based efficient usable security solutions for body sensor networks,” *ACM Transactions on Sensor Networks*, vol. 6, no. 4, pp. 31-64, July, 2010. [Article \(CrossRef Link\)](#).
- [23] J. Zhou, Z. Cao, X. Dong, N. Xiong and A.V. Vasilakos, “4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks,” *Information Sciences*, vol. 314, pp. 255-276, September, 2015. [Article \(CrossRef Link\)](#).
- [24] U.C. Niranjan, S.S. Iyengar, N. Kannathal and L. C. Mina, “Simultaneous storage of patient information with medical images in the frequency domain,” *Computer methods and programs in Biomedicine*, vol. 76, no. 1, pp. 13-19, October, 2004. [Article \(CrossRef Link\)](#).
- [25] D.C. Lou, M.C. Hu and J.L. Liu, “Multiple layer data hiding scheme for medical images,” *Computer Standards & Interfaces*, vol. 31 no. 2, pp. 329-335, February, 2009. [Article \(CrossRef Link\)](#).
- [26] M. Ulutas, G. Ulutas, V.V. Nabiyev, “Medical image security and EPR hiding using Shamir's secret sharing scheme,” *Journal of Systems and Software*, vol. 84, no. 3, pp.341-353, March, 2011. [Article \(CrossRef Link\)](#).
- [27] N.A. Memon, S.A.M. Gilani, A. Ali, “Watermarking of chest CT scan medical images for content authentication,” *In Int. Conf. on Information and Communication Technologies*, pp. 175-180, August 15-16, 2009. [Article \(CrossRef Link\)](#).
- [28] S. Rawat and B. Raman, “A blind watermarking algorithm based on fractional Fourier transform and visual cryptography,” *Signal Process*, vol. 92 no. 6, pp. 1480–1491, June, 2012. [Article \(CrossRef Link\)](#).
- [29] B. Surekha, G.N. Swamy and K.R.L. Reddy, “A novel copyright protection scheme based on Visual Secret Sharing,” in *Proc. of 3rd Int. Conf. on Computing Communication & Networking Technologies (ICCCNT)*, pp. 1-5, July 26-28, 2012. [Article \(CrossRef Link\)](#).
- [30] T.R. Singh, K.M. Singh and S Roy, “Video watermarking scheme based on visual cryptography and scene change detection,” *AEU-International Journal of Electronics and Communications*, vol. 67, no. 8, pp. 645–651, August, 2013. [Article \(CrossRef Link\)](#).
- [31] M. Naor and A. Shamir, “Visual cryptography,” *Advances in Cryptology-EUROCRYPT'94 Lecture Notes in Computer Science*, vol. 950, pp. 1-12, May 23, 2006. [Article \(CrossRef Link\)](#).
- [32] CrossBow, MICAZ datasheet, 2010. Available: [Article \(CrossRef Link\)](#).
- [33] Sparkfun, “Pulse Sensor SEN-11574.” Available: [Article \(CrossRef Link\)](#).



Xiyao Liu was born in Hunan Province, in 1987. He received the B.S. degree and the Ph.D. degree from School of Electrical Engineering and Computer Sciences, Department of Microelectronics, Peking University in 2008 and 2015. He is now a lecturer in School of Information Science and Engineering, Central South University, Changsha, China. His research interests include security of sensor networks, multimedia technology and digital signal processing.



Yuesheng Zhu received his B.Eng. degree in Radio Engineering, M.Eng. degree in Circuits and Systems and Ph.D. degree in Electronics Engineering in 1982, 1989 and 1996, respectively. He is currently working as a professor at the Lab of Communication and Information Security, Shenzhen Graduate School, Peking University. He is a senior member of IEEE, fellow of China Institute of Electronics, and senior member of China Institute of Communications. His interests include digital signal processing, multimedia technology, communication and information security.



Yu Ge is a scientist in the Institute for Infocomm Research (I²R), A-Star, Singapore. She received her M.Eng. and Ph.D. degrees from National University of Singapore and Nanyang Technological University respectively, all in wireless communication networks area. She joined I²R in 2001 and worked in various research areas including VoIP in heterogeneous wireless networks, wireless mesh/ad hoc networks, and wireless sensor networks. She is currently leading a research team in the area of wireless body area networks (WBANs) for human-centric sensing. Her current research interests are transmission and sensing technologies in wireless communication networks for end-to-end human-centric service provisioning.



Dajun Wu received the B.S. degree in computer science from Northwest University, Xi'an, China, and the M. Eng. degree in computer engineering from Xi'an Jiaotong University, Xi'an, China, in 1993 and 1998, respectively. From 1998 to 2000, he was a Research Scholar in the School of Computer Engineering, Nanyang Technological University, Singapore. In 2007, he obtained the Ph.D degree in electrical and computer engineering from National University of Singapore. Since 2000, he has been with Institute for Infocomm Research, Singapore. His research field includes multi-media coding/transmission and sensor networks.



Beiji Zou received the B.S. degree in Computer Science from Zhejiang University, China, in 1982, received the M.S. degree from Tsinghua University specializing CAD and computer graphics in 1984, and obtained the Ph.D. degree from Hunan University in the field of control theory and control engineering in 2001. He is now a professor in School of Information Science and Engineering, Central South University, Changsha, China. He has published more than 100 papers in international conferences and journals. His research interests include computer graphics, computer vision, multimedia processing and mobile health.