An Energy Conservation Authentication Scheme in Wireless Body Area Network

Chin-Chen Chang[1], Jung-San Lee[1,*], and Jia-Shang Wu[2]
[1]Department of Information Engineering and Computer Science,
Feng Chia University, Taichung, Taiwan, R.O.C.
[2]Department of Computer Science and Information Engineering,
National Chung Cheng University, Chiayi, Taiwan, R.O.C.

Abstract

Wireless Body Area Network (WBAN) is an important branch which takes the advantage of the wireless sensor network (WSN) to achieve the corresponding goal in remote healthcare application. Security of WBAN is no doubt a crucial issue while developing telecare medical system. However, high computational costs and energy consumption are required in current mechanisms to confirm the security of communication protocol. Thus, we aim to propose a lightweight version based on symmetric cryptography, xor operation, and one way hash function in guaranteeing the security problem. We have simulated the system according to the NS-2 simulator. The experimental results have demonstrated that the proposed method is superior to related works in terms of energy consumption and communication costs.

Keywords: WBAN, energy consumption, authentication, NS-2

1. Introuduction

Wireless Sensor Network (WSN) [1] has become a popular technique due to the rapid growth of computer science technology. With the advancement of the WSN technique, many applications can be improved, like field studies, the military, transportation, amusement, gaming and even healthcare, making it easier to gather more data. One high-profile area is the Wireless Body Area Network (WBAN). WBAN [9] is an important area that takes advantage of the WSN, and achieves corresponding goals in remote healthcare applications.

A WBAN system provides remote healthcare applications for monitoring patients. This means that if WBAN is available, the system provider (e.g., the doctor or the hospital) can gather the patient's personal information such as heartbeat, blood pressure, etc. The system provider places wearable sensors or implant sensors on the patient to gather the personal information, and the patient will no longer need to meet with the doctor as often. Usually, the gateway devices would be a portable device like a mobile phone. Zigbee or some other devices that support short-distance transmissions can satisfy the requirement. Once the

WBAN system is available, the gateway will be able to gather the data from sensors and send it back to the system provider. Figure 1 shows a typical example of a WBAN pathway.

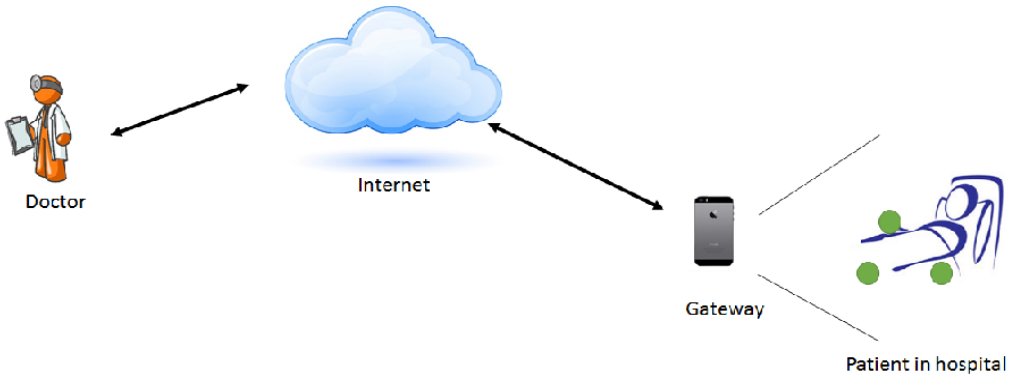


Figure 1. A WBAN remote healthcare example; the gateway gathers the data and sends it back to the doctor.

WBAN faces several kinds of challenges, and one of them is security. Making sure the patient data being transmitted from the internet is secure is the most important aspect. WBAN relies on mobile devices and sensors, which are resource-constrained in terms of power, memory, communication rate and computational capability, and as such, security solutions proposed for other networks may not be applicable to WBANs. Authentication, integrity and data freshness together with availability and secure management are the main security requirements in WBAN. Our solution provides WBAN systems with authentication between the patient gateway and the system provider. We proposed a hash- and xor-based authentication protocol to ensure data security when transmitting data. This method not only reduces the computation times, but also communication times and the energy costs, and it can be easily implemented through mobile devices and sensors as compared to other protocols.

The latest international standard for WBAN is the IEEE 802.15.6 standard, which provides an international standard for the purposes of low power, short range and extremely reliable wireless communication with the human body, and supports a wide range of data rates for many kinds of applications. IEEE 802.15.6 also defines three levels of security. Level 0 is unsecured communications, level 1 is authentication only and level 2 is authentication and encryption. In the WBAN system, all of the devices must select a level during the association process. A pre-shared master key (MK) is activated in a unicast communication. A pairwise temporal key (PTK) is generated for only one use per session. A group temporal key (GTK) is generated and shared with the corresponding group in a multicast communication. All of the devices in the WBAN system must go through certain stages at the MAC layer before exchanging data.

A typical WBAN system looks like [8] and [14]. Thanks to the gift of computer technology, it is easy to implement. Short-distance transmission protocol like zigbee in IEEE 802.15.4 standard is suitable for the WBAN environment. With the rapid growth of the sensor technology, more and more applications can be created for various uses. Sensors and other embedded devices have made it affordable and easier to model the WBAN system [2][5][15]. But as we mentioned before, the WBAN system may encounter security problems. When data is transmitted from the patient through the internet from far away, it will face the risk of being stolen or tampered with. Therefore, authentication between patients and the system provider is important. User authentication is the basis for most types of access control, along with other security fundamental purposes like user accountably. In 1981, Lamport introduced the concept of the remote authentication protocol to ensure the security of the communication channel [10]. The public key infrastructure (PKI), including each party's public and private key and a corresponding public key certificate that has been issued by a semi-trusted certificate authority (CA), should be checked every time authentication is required. Some projects subsequently have proposed combining the digital certificate and remote authentication protocols together [7][17][18].

ID-based cryptography was first proposed by Adi Shamir [16]. ID-based cryptography is a type of public-key encryption in which the public key of an owner is unique information about the identity of the user (e.g., the user's identity code). ID-based cryptography allows any party to generate a public key from a known identity value. A trusted third party, often called the private key generator (PKG), generates the corresponding private keys. Some additional research has been performed to try to specifically solve the authentication problem in WBAN [6][12][20]. Cao et al. [3] proposed their authentication scheme in 2009. Their authentication scheme makes use of identity-based signatures and computing methods like hash, pairing and scalar multiplication. The author focuses on the signature generation and verification with an identity-based method. Some authentication protocols are based on hash and xor operations, like [4], which is faster and more energy efficient compared to the authentication protocols based on other techniques, reducing resource consumption. Our research is based on hash and xor operation to provide secure communication. Compared to other competitors, our protocol saves energy and provides security while transmitting data.

The rest of the paper is organized as follows, Section 2 introduces background on WBAN settings and cryptographic primitives. Section 3 presents our protocol. Security analysis is shown in section 4. Section 5 presents our experimental results. Finally, we make conclusions in section 6.

2. Related works

Recently, the authentication of WBAN has been widely discussed. An enormous number of works incorporating security features in the Wireless Body Area Network applications have been proposed, and each scheme has its own merits and demerits.

Liu et al.[12] discussed their certificateless signature (CLS) scheme, which is computational, efficient and provably secure against existential forgery on adaptively chosen message attacks in the random Oracle model. Different from [20], Hu designed a WBAN protocol in a cost effective and certificateless way, and it improves the scheme in [3]. The protocol in [20] provides the WBAN security base on pairing, elliptic curve cryptography and signature scheme, though both protocols [12] and [20] are too cost intensive on computation and communication. This is not practical because embedded devices are usually resource constrained, but these protocols do over-consume resources. For example, (1) protocol [12], [20] do many computations, especially pairing and scalar multiplication, while authenticating. Both of them use more hardware resources than other kinds of computations. (2) Some protocols transfer the data through a network manager. This is a waste of time and energy. Therefore, to reduce the waste of resources in a resource-limited surface, we have to restrict the use of the computation methods. He et al.[6] proposed a secure, lightweight, confidential and denial-of-service-resistant data discovery and dissemination protocol for WBAN using xor operation and hash. They used a key hash chain to guarantee the security of their protocol, and they also did the design and implementation. However, this method faces a forward secrecy problem because it uses a multiple one-way key hash chain.

In another study, Li and Hong[11] proposed a WBAN authentication scheme in a certificateless scheme. But they provide a revocation scheme for the user. Their revocation is based on remembering a variable of expiration date (E.D). With this variable, it can achieve the revocation method by revoking the admission of the device if the E.D is due.

Different from these studies, in this paper we present our own authentication scheme. Because the need of WBAN security is growing and the influence between efficiency and security is still a trade-off, our proposed protocol tries to find a solution for both issues.

3. Proposed methods

In this section, we will introduce the proposed methods of the protocol. Then, we provide the system model and the objectives.

3.1 Notations

Table 1 describes the notations used throughout the paper.

Table 1. Notations

Notation	Description
PW	The password of the device in WBAN.
ID	The identity of the device in WBAN.
X	The random number generated by the system.
r	The random number generated by the system.
T	The timestamp in WBAN.
Sk	Special secret key.
msg	The delivered message.

3.2 System Model

In Figure 1, we showed our system model. In this section, we will introduce our system precisely. Consider a system provider (SP), like the doctor in the hospital, who has constructed the system. The doctor and hospital need to guarantee the security of the patient's data, as proposed by the WBAN system. Most of the time, the SP refers to a computer or a server. The SP can ask for the patient's personal data through the internet, and can also send back some parameters to update the nodes in system. In this way, the patient (client) far away from the SP will be monitored remotely. For each WBAN, body sensors are used to automatically monitor physiological readings, which can be forwarded to a nearby processing device. The patient usually uses wearable sensors and implanted sensors, through which their data will be gathered by the processing device near them, which we call the gateway node (GN). The GN is an intermediate node responsible for receiving and sending the data bidirectionally. The GN can be a mobile device, like a phone.

3.3 Overview

In this section, we will introduce our authentication protocol. The system workflow is in Figure 2.Our scheme secures the network communication path between the doctor in hospital

and the far away patient. The design principle of our protocol is lightweight and efficiency in authentication. To prevent the WBAN from intruders, our protocol use a one-way hash and xor operations to secure the secret information, including the secret key, identity and a random number. Based on the symmetric c ryptosystem in the secret key, our protocol reduce encrypts the message with confidentiality. We describe our authentication protocol in two parts: authentication and key refresh. As Figure 2 shows, our protocol does registration and authentication procedures. Currently, we use a network simulator, NS-2, to simulate our project. However, a doctor may have more than one patient. This means that he could propose more than one similar WBAN, so that the identity of registration will be different to recognize each patient. All the patients with their gateway devices can run the authentication protocol to guarantee the data confidentiality.

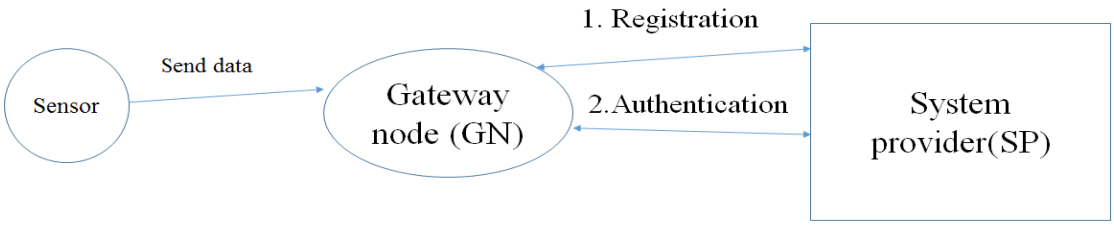


Figure 2. The workflow in the proposed protocol.

3.4 Authentication protocol

The authentication protocol involves three entities, SP (system providers), GN (gateway nodes) and sensors, and it consists of the initialization phase, registration phase and the authentication phase.

Initialization phase: Before the WBAN system is set up, every device in the WBAN has to preload a random password (*PW*), a unique identity (*ID*), a random number X and a random number seed s for the random number generator *F*. Then, the one-way hash function H is set up in every device. Once these phases are complete, the WBAN system is set up. Here, the SP records all the personal information of the devices.

Registration phase: To confirm the nodes we have planted, our protocol first registers it. The sensor node uses its *PW*, *ID* and random number *X* to calculate $H(PW)$, $H(ID||X)$ and stores the value of $H(PW) \oplus H(ID||X)$. Considering that SP knows all the IDs in the WBAN, SP can calculate and store $H(ID||X)$.

Authentication phase: While the authentication starts, the devices are transmitting the patient's data to the server. When the GN gets the message from the device, the GN authenticates with SP by performing the following steps.

(a) GN generates T and sends it with the ID to SP.
(b) SP checks if $H(ID_{GN}||X)$ holds.
(c) If available, SP calculates $Sk = H(H(ID_{GN}||X)||T)$ and sends back $H_{Sk}(T)$ to GN.

Once the GN receives the value $H_{Sk}(T)$ from SP, GN will do the XOR operation with the hash value previous stored and the hash value of the input password, and checks if it can get the hash value of the $H_{Sk}(T)$ using the steps below. If the hash value of the ID and X are not the same, then it refuses the authentication; else, it sends the encrypted message back to the SP.

(a) If $H(PW)\oplus H(ID||X)\oplus H(PW)||T == H_{Sk}(T))$.
(b) Encrypt the message by AES-128bit $E_{Sk}(msg)$.
(c) Send $E_{Sk}(msg)$.

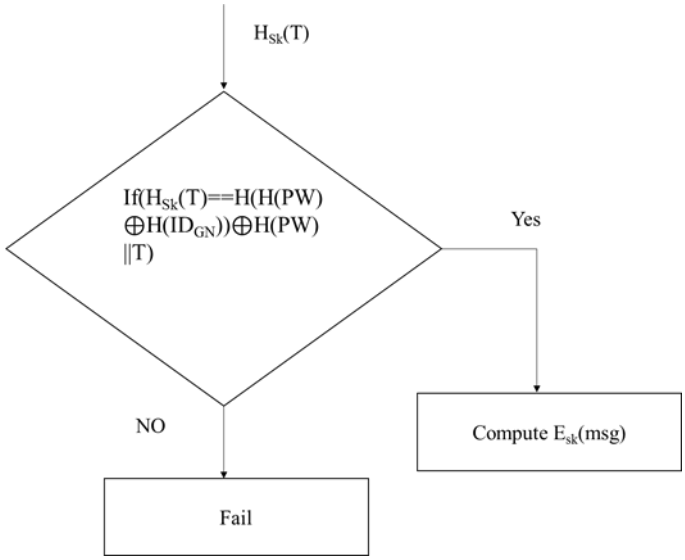


Figure 3. The flow chart of the authentication.

Our sensors on patients send the sensor id, S_{id}, then deliver the data and timestamp $p = <S_{id}, data, T>$ after authentication.

3.5 Key refresh scheme

Our main purpose is to protect the data security when in transmission. The symmetric encryption method AES provides the security of our message. In this project, we choose the standard AES because the resource of the embedded device is limited. The cost of AES is less than other encryption methods like ECC and RSA. Considering that the resource is

constrained in embedded devices on patients, this method is more suitable than others. If our secret key is exposed, the system will no longer be safe. We have to change the 128-bit random number key periodically to ensure the safety of authentication. In this way, the random number key generator F is pre-shared in every node. We trigger the key refresh step for every so often to generate a new random number key for the encryption.

We use an AES 128-bit random number key to provide the security of the encrypted message. By running F with seed s, all nodes will simultaneously update the random number key. To ensure the security of the encrypted message, our system has to change the random number 128-bit secret key for the encryption a few times per day. We refresh the random number seed every 8 hours. We have pre-shared parameters, and the random number generator F in every node in the WBAN system. When the WBAN system is going to refresh the secret key, it will trigger the random number generator to generate the secret key. Because the seed is the same, the random number generator is the same. Therefore, we can get the same secret key on every node simultaneously. At last, we finish the key refresh step.

4. Security analysis

In this chapter, we analyze the security of our protocol. As the flow chart shows in Figure 3, our authentication protocol ensures the security between the GN and the SP. Our scheme is based on the assumptions below.

Assumption 1: The block cipher is a secure pseudorandom function (PRF) family. Note that our scheme uses a block cipher with a cipher block. Block ciphers can achive security by using PRF.

Assumption 2: The block cipher is semantically secure. Note that in our scheme the block cipher can be implemented by advanced encryption standard (AES).

Assumption 3: The hash function is a cryptographic hash function. Note that in our scheme the hash function $H(.)$ satisifies three properties, including pre-image resistance, second pre-image resistance and collision resistance. These three propertities are described below.

Preimage resistance: For any given hash value h, it is computationally infeasible to find b such that $H(y) = h$.

Second pre-image resistance: For any given block x, it is computationally infeasible to find y $\neq$ x with $H(y) = H(x)$.

Collision resistance: It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$.

First, the registration phase requires a unique identity (ID) and password (PW) and a random

number (X). Our protocol stores these values after they are hashed. Then, the authentication phase checks if the hash value of the ID, X and the timestamp T is correct or not. At last, our message is sent after the encryption of the AES 128-bit random number key.

To analyze these security issues, consider the surface of IEEE 802.15.6 standard in a level 2 surface, which provide data rates up to 10 Mbps, while simultaneously complying with strict non-interference guidelines where needed. In order to modify the packets in the WBAN system, an intruder has to gain control of the embedded device in the system, or under the guise of the legal device to compromise the secret message for controlling the whole system.

The following sections list the main progress of the protocol and discuss the resilience against possible attacks. Here, we list some possible attacks including a replay attack, denial-of-service, Masquerade attack and password guessing.

4.1 Replay attack

Consider that the intruder plants a fake device in the system as a pretend gateway, or a body sensor for eavesdropping on the message for the purpose of paralyzing the WBAN. The device must be planted in the communication link between the SP and sensor nodes. There are two possible scenarios.

(1) The intruder device is set between the GN and SP, and the replay attack will happen when the GN sends the requested message back to the SP or when the SP sends the message to the GN. In the proposed scheme, while the GN is requested, it responds back with p = $<ID_{GN}, T>$. Following the authentication step in section 3, the intruder resends p = $<ID_{GN}, T>$. The verification of the replayed message cannot be passed due to the time interval $(T_2 - T) > \Delta T$ at the device. ΔT means a mutually agreed transmission delay between the legal entities, and the receiver (device A) will reject the message. Moreover, the hash value of T will not be the same due to the collision resistance of the assumption 3, as we can not find any pair (T_1, T_2) such that $H(T_1) = H(T_2)$.

(2) Intruder device gets the message from the patient sensors. It replays the message to the GN, and the replay attack happens at that moment. Our proposed method counters this problem by timestamp. When the intruder gets p = $<S_{id}, data, T>$, it then responds with p = $<S_{id}, data, T>$ to the gateway after it receives the packet from the device in the WBAN. The verification will not be passed due to the time interval $(T2 - T) > \Delta T$ at the device. ΔT means a mutually agreed transmission delay between the legal entities, and the receiver (device A) will reject the message.

4.2 Denial of service

Suppose that the intruder, John, wants to do a Denial of Service (DoS) attack on the WBAN system. He will need to control some of the embedded devices first, which means he has to hunt down some of the devices. He launches a DoS attack by replaying an old message. However, our system proposed in this paper can resist the attack. As described in section 3, the proposed approach exploits the advantages of timestamps. If the messages are sent too frequently, it will be thought of as a DoS attack. In addition, our system achieves mutual authentication, so it is not able to do authentication simultaneously. Illegal transmission through the device will be turned down by the SP.

4.3 Masquerade attack

An attacker cannot masquerade as the legal entity between the SP and the device to join in the smart home network. Since the SP has made a list of the identities of the legal devices, intruders are not going to pass the verification when authenticating.

Suppose that an intruder wants to trigger a Masquerade attack using an illegal device. It must send p = <*ID*, *T*> to the SP for registration and try to spoof SP. SP will check the $H(ID||X)$ and verify whether it is legal. Because the registration step needs the hash value of ID and random number *X*, the intruder will not pass verification because it doesn't have *X* and Assumption 3 of the secure cryptography hash function. As long as the verification is not passed, the authentication will not start. The illegal device won't be able to get the authorization for the WBAN system. Therefore, the intruder must intercept a legal device's packet. Because our protocol delivers the *ID* and *X* after it executes the hash, the intruder can't get a verified legal identity. The intruder must know how to compute the hashed value, or he can't get the real *ID* and *PW*. If the intruder gains access with the SP, it still can't get the message because of Assumptions 1 and 2. Since we have used the secure block cipher to generate AES, our message is not going to be exposed.

4.4 Password guessing attack

We have used the *PW* in the registration and authentication phases. An intruder, John, may do a password guessing attack, like brute force and dictionary attacks. Both brute force and dictionary attacks try to get the password for authentication. However, this method won't be successful because of Assumption 3. We use a secure cryptographic hash to protect our password during authentication. Regardless of brute force attacks and dictionary attacks, they

won't be able to gain access to the *PW*. In addition, if the intruder gets *PW* and authenticates with SP, it still can't get the message because of Assumptions 1 and 2. We have used a secure block cipher to generate AES, so our message will not be exposed.

5. Experiment results

5.1 Experiment

The section discuss the experiment performance of the proposed scheme, and then compares with [6][12][20]. Our experiment mainly aims at three parts, computation communication and energy cost. Figure 4 stands out to be the simulation of our experiments with the network simulator NS-2. Node zero represents the SP, and the other 10 nodes represent ten different patients far away. While doing authentication for a specific patient, the gateway node does the authentication with the corresponding gateway node. If multiple gateway nodes are doing authentication, the SP will perform the authentication from the smallest ID to the largest. The WBAN system can be implemented by the usage of famous embedded devices like MicaZ or TelosB.

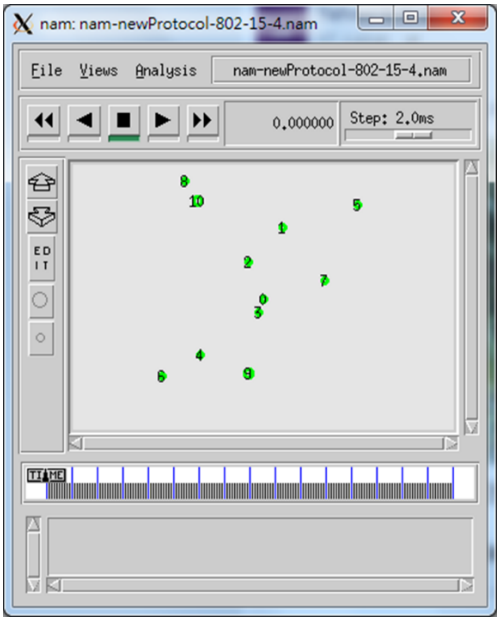


Figure 4. The simulation done by NS-2 of our protocol with 10 nodes and a sender (0).

5.2 Analysis

In this section, we evaluate the performance of our proposed protocol in terms of computation costs, communication costs and energy cost. Table 2 shows the computation cost comparison of the other WBAN protocols [6], [12] and [20] and our protocol. Assumptions are that the system has one sensor on the patient, one gateway near the patient and the server is far from the location of the patient.

Table 2. Computation cost for the other WBAN protocols and our protocol.

	ours	[6]	[12]	[20]
SP	$1T_{Hash}$	$1T_{Hash}$	$2T_{Sm}+1T_{Bp}+2_{Hash}$	$4T_{Hash}+3T_{Sm}+1T_{Xor}$
Patient Gateway (GW)	$3T_{Hash}+1T_{Xor}$	$1T_{Hash}$	$2T_{Hash}+2T_{Sm}+1T_{Exp}$	$3T_{Hash}+2T_{Sm}+1T_{Xor}$
Patient sensor		$1T_{Hash}$		
Total	$4T_{Hash}+1T_{Xor}$	$3T_{Hash}$	$4T_{Hash}+4T_{Sm}+1T_{Bp}+1T_{Exp}$	$7T_{Hash}+5T_{Sm}+2T_{Xor}$
Time (ms)	135.85	91.58	466.74	318.63

Table 3 lists the simulation time of the operation [3]. We can see that the simulation in [3] tell us that it takes more time while doing pairing, scalar multiplication and exponentiation operation. As a result, this operation takes more computing resources while performing pairing and exponentiation operations on the server or client side.

Table 3. The operation simulation result in

Operation	Server (ms)	Client (ms)
Modular exponentiation	13.21	192.38
Scalar multiplication	6.38	92.91
Hash	3.04	44.27
Pairing	20.04	

Let T_{Hash}, T_{Xor} , T_{Bp} , T_{Sm} , and T_{Exp} in Table 2 be the time for performing the hash operation, xor operation, bilinear paring, scalar multiplication and exponential operation, respectively. In [3] and [19], we can get the simulation time of these operations on the computer in Table 2.

Embedded devices on the patient spend more time on computing than the server due to the required computing resources, so reducing the computation cost especially on the patient side is a must. Because T_{Xor} is very small compared to other operations, we can neglect it when computing the communication time. In Table 2, we see that our authentication protocol takes 4 hashes and 1 xor operation in one time. Protocol [12] and protocol [20] take too many computations compared to our protocol. Protocols [6] make use of the public key primitives.

This implies that the existence of some authority mechanisms, such as the certificate authorities that generate and certify cryptographic keys for different purposes. This means that more computation resources are needed to guarantee the safety of the WBAN. Protocol [20] makes use of the partial private key technique to build a scalable and certificateless authentication protocol. Because of the partial key, both parts have to use more resources for computing to compute the real key. This takes more time and resources than to simply use a hash chain to secure the key for authentication [6]. Still, every node has to do a one-way hash function. Our protocol is based on hash and xor operations, and the computation cost of our protocol is less than protocols [12] and [20], but a little more than protocol [6].

Here, we take two common embedded devices as examples. We have to determine the energy models of the embedded sensors of MICAz and TelosB, which we later use, to estimate and analyze the energy consumption of cryptographic protocols. The MICAz is based on a low-power 8-bit microcontroller, ATmega128L, with a clock frequency of 7.37 MHz. The TelosB features the 16-bit MSP430 microcontroller running at 4 MHz. Both nodes run TinyOS and have embedded an IEEE 802.15.4 compliant CC2420 transceiver with a claimed data rate of 250 kbps. These two embedded devices are commonly used in WBANs.

Table 4 is the energy cost table [13] in encryption, which is the energy cost while doing the cryptography method per time. Table 5 shows the energy cost while the sensor sends and receives, for the MICAz and TelosB [13]. While authenticating, ECC can be used in a large number of cryptographic primitives based on bilinear mappings on various elliptic curve groups. AES is used in securing the message. Because these two are the main cryptography methods, we can analyze the main energy cost using Table 4, and we can estimate the energy consumption during transmission using Table 5.

Table 4. Estimated energy costs of cryptographic operations for the MICAZ and TELOSB

Energy cost	MICAz	TelosB
AES-128 128-bit encrypt	38μJ	9μJ
ECC-160 point mult	55mJ	17mJ

Table 5. Energy costs of common operations on the embedded device.

Energy cost	MICAz	TelosB
Transmit 1 bit	0.60 μJ (170)	0.72 μJ (600)
Receive 1 bit	0.67 μJ (190)	0.81 μJ (680)

To implement a WBAN system, using the data in Tables 4 and 5, we can get the system structure, using Figure 5. Figure 5 is an example model of a WBAN. We construct the WBAN system in an embedded device platform. The end user wears an embedded device like TelosB

and MicaZ, and these sensors send data to the gateway, which can also substitute for the switch or mobile phone using embedded devices. Note that in the structure of Figure 5, we can easily calculate the energy consumption. Our protocol and [6] use AES 128-bit encryption to provide security of the delivered message. The main cryptographic energy cost is 38 and 9μJ, depending on the device.

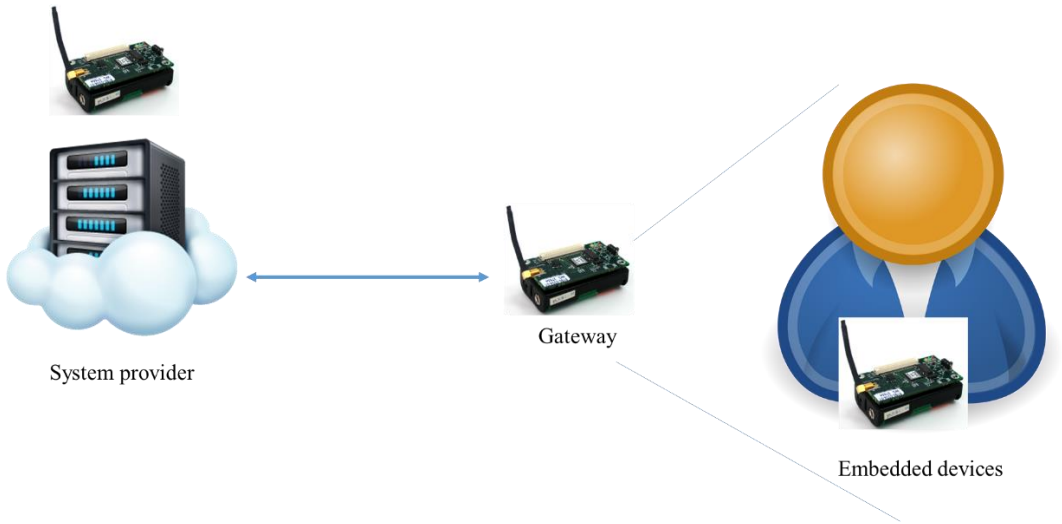


Figure 5. A WBAN system structure in an embedded platform.

In addition, we calculate for our proposed protocol. Considering the energy consumption of the sum of the embedded sensors on the patient and the gateway, we compute the energy consumption of our proposed protocol with Table 5 and Table 6. Table 6 shows the simulation with one time of the energy cost. All of our elements are 12 bytes, including the IDs as 4 bytes, timestamp as 4 bytes and the element after being hashed is 20 bytes. Here, we estimate all the protocols in the SHA-1 hash function. Our estimated energy data is calculated as below.

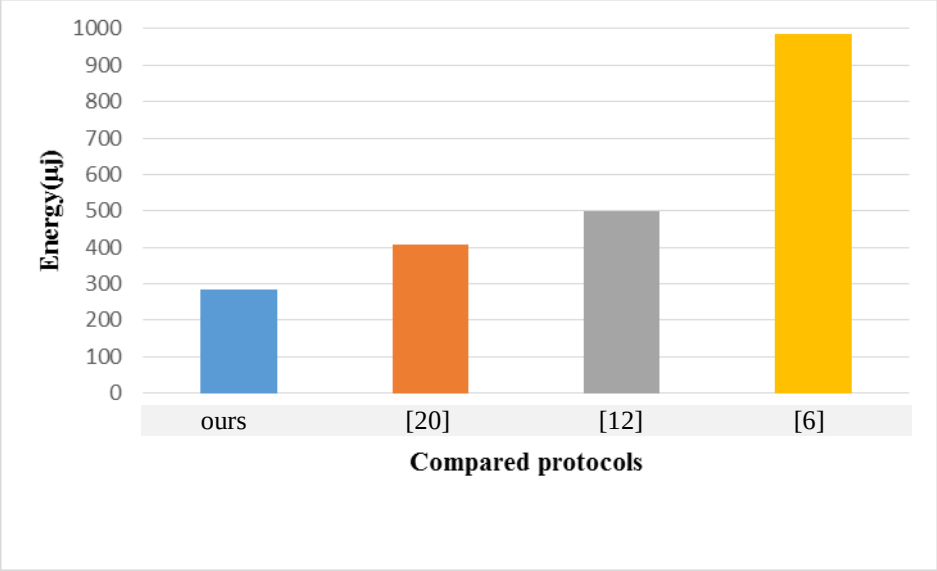
Table 6. The energy cost of our protocol while communication.

Message at device (bits)	Energy costs (in μJ) (Micaz)	Energy costs (in μJ) (TelosB)
Send by SP (64)	38.4	46.08
Receive by GN (64)	42.88	51.84
Send by GN (160)	96	115.2
Receive by SP (160)	107.2	129.6
Total energy required	284.48	342.72

Let us take the MicaZ as an example. In section 3, Figure 3, we explained the authentication phase, and we discussed the size of our elements in the preceeding paragraph. The first 64 bits come from the phase when the GN sends the ID_{GN} (4 bytes) and T (4 bytes)

to SP. The later 16 bits from SP is the hashed value of the timestamp while doing the implementation. Table 5 tells us the energy cost while MicaZ is transmitting and receiving the message. Calculating the total energy requirement, we just have to multiply the transmitted bits and the corresponding energy consumption. Thus we can get the experiment results in Table 6. Following this rule, we analyzed the energy consumption in [6], [12] and [20]. In [6] we create the hash chain each time of message transmission, and we analyzed the size of the transmitted packet. The overall size is 388 bits (order: 4 bits; key: 2 bytes; version: 4 bytes; data: 2 bytes, and the two hashed keys generated by SHA-1 are 320 bits). In this way, we can get the estimated energy by summing up the transmission and received packet size. The authentication protocol in [12] and [20] accomplish the authentication with many parameters like timestamp, random number and message. We simulate the type int (4 bytes) and char (1 bytes). To sum up, we calculated the simulation communication energy cost for MicaZ in Table 7.

Table 7. Communication energy cost while the message exchanging.



Though the practical cost depends on the operation during authentication, it is efficient to end the authentication by doing less message exchanges and less computing.

6. Conclusions

In this paper, we proposed a lightweight authentication protocol to guarantee the safety of the WBAN. Our protocol is based on hash and xor operations and does fewer steps than the

other compared WBAN protocols. The cost of message encryption that is based on symmetric cryptography saves more energy than other methods. In a resource-constrained WBAN, using a protocol based on symmetric cryptography is more likely. It is suitable for use on resource-constrained embedded system surfaces as compare to other protocols. We prove that the competitive protocols based on pairing and hash chains are not efficient. Therefore, we have shown that our scheme provides security in WBANs and saves resources on the embedded devices.

References

[1] I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102-114, 2002.

[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, 2009.

[3] X. Cao, X. Zeng, W. Kou and L. Hu, "Identity-based anonymous remote authentication for value-added services in mobile networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3508-3517, 2009.

[4] C.C. Chang and H.D Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Transactions on wireless communications*, vol. 15, no. 1, pp.357-366, 2016.

[5] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao and V.C.M. Leung, "Body area networks: A survey," *Mobile Networks and Applications*, vol. 16, pp. 171-193, 2011.

[6] D. He, S. Chan, Y. Zhang and H. Yang, "Lightweight and confidential data discovery and dissemination for wireless body area networks," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 2, pp. 440-448, 2014.

[7] M.S. Huang and L.H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28-30, 2000.

[8] E. Jovanov, A. Milenkovic, C. Otto and P.C. de Groen, "A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation," *Journal of NeuroEngineering and Rehabilitation*, vol. 2, no. 1, 2005.

[9] K.S. Kwak, S. Ullah and N. Ullah, "An overview of IEEE 802.15.6 standard," *Proceedings of the 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies*, pp. 1-6, 2010.

[10] L. Lamport, "Password authentication with insecure communication," *Communications*

of the ACM, vol. 24, pp. 770-772, 1981.

[11] F. Li and J. Hong, "Efficient certificateless access control for wireless body area networks," *IEEE Sensors Journal*, vol. 16, no. 13, pp. 5389-5396, 2016.

[12] J. Liu, Z. Zhang, X. Chen and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 332-342, 2014.

[13] G. Meulenaer, F. Gosset, F. X. Standaert and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," *Proceedigns* of *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 580-585, 2008.

[14] A. Milenkovic´, C. Otto and E. Jovanov, "Wireless sensor networks for personal health monitoring: Issues and an implementation," *Computer Communications*, vol. 29, pp. 2521-2533, 2006.

[15] M. Seyedi, B. Kibret, D.T.H. Lai and M. Faulkner, "A survey on intrabody communications for body area network," *IEEE Transactions on Biomedical Engineering*, vol. 60, no. 8, pp. 2067-2079, 2013.

[16] A. Shamir, "Identity-based cryptosystems and signature schemes," *Proceedings of Advances in Cryptology*, vol. 196, pp. 47-53, 1984.

[17] U. Uludag, S. Pankanti, S. Prabhakar and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948-960, 2004.

[18] T. Weigod, T. Kramp and M. Baentsch, "Remote client authentication," *IEEE Security and Privacy Magazine*, vol. 6, no. 4, pp. 36-43, 2008.

[19] Q. Xie, D. Hong, M. Bao, N. Dong and D. S.Wong, "Privacy-preserving mobile roaming authentication with security proof in global mobility networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 5, 2014.

[20] H. Xiong, "Cost-effective scalable and anonymous certificateless remote authentication protocol," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2327-2339, 2014.

Author Biography

Chin-Chen Chang received his BS degree in applied mathematics in 1977 and his MS degree in computer and decision sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D in computer engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. From 1989 to 2004, he has worked as a professor in the Institute of Computer Science and Information Engineering at National Chung Cheng

University, Chiayi, Taiwan. Since 2005, he has worked as a professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. Dr. Chang is a Fellow of IEEE, a Fellow of IEE and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, and the Phi Tau Phi Society of the Republic of China. His research interests include computer cryptography, data engineering, and image compression.

Jung-San Lee received the BS degree in computer science and information engineering from National Chung Cheng University, Chiayi, Taiwan in 2002. He received his Ph.D. degree in computer science and information engineering in 2008 from National Chung Cheng University, Chiayi, Taiwan. Since 2008, he has worked as an assistant professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. His current research interests include electronic commerce, information security, cryptography, and mobile communications.

Jia-Shang Wu received his BS degree in 2016 from National Chung Cheng University, Chiayi, Taiwan. His current research interests include information security and sensor networks.