Liu *et al. EURASIP Journal on Wireless Communications and Networking* (2015) 2015:188
DOI 10.1186/s13638-015-0406-2

EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Efficient authenticated key exchange protocols for wireless body area networks

Jingwei Liu[*], Qian Li, Rui Yan and Rong Sun

Abstract

Secure protocol is a vital guarantee in all kinds of communication network environment. Designing on authenticated key exchange protocols is a hotspot in the field of information security at present, and the related theories have been increasingly mature. However, there is still scarcely any appropriate security protocol to guarantee the communication security of wireless body area networks (WBANs). In this paper, according to the standards on WBAN, we define a layered network model in accordance with the definition of two-hop star network topology firstly. In line with this model, we put forward two new authenticated key exchange protocols based on symmetric cryptosystem, which are suitable for WBAN application scenario. The proposed protocols support the selective authentication between nodes in WBAN. Simultaneously, two pairs of session key are generated efficiently and succinctly in each certification process. Finally, after security analyzing and performance evaluating demonstrate that the proposed key agreement protocols are proved to meet desired security properties with light computation and communication overhead. The proposed protocols provide a primitive to develop efficient and secure WBAN systems.

Keywords: Security protocol; Wireless body area network; BAN logic; AES

1 Introduction

Authenticated key exchange protocols are important and have been widely applied in network communication. By a pre-registration, two communication parties share a secret symmetric key with a trusted server correspondingly. When the two participants try to exchange any information with authentication property confidentially in an insecure environment, they must be in agreement on a new secret session key by the help of a server. This kind of key exchange method is called three-party authenticated key exchange (3PAKE), and the 3PAKE protocols typically are employed for mutual authentication and secure communication in various applications.

A good design of 3PAKE protocols should meet various security requirements of different applications, which are described as follows.

- Mutual authentication: The participants of protocols should be authenticated by the server and also they must be authenticated each other by themselves.
- Session key security: The agreed session key should only be known by parties who participate in communication process.
- Perfect forward secrecy: Perfect forward secrecy is the property that a session key derived from a set of long-term keys will not be compromised if one of the long-term key is compromised in the future.

In recent years, many three-party authenticated key exchange protocols have been proposed [1–10] in recent years. Yeh et al. [4] proposed two 3PAKE protocols for secure communication over a public network. One was a plaintext-equivalent authentication protocol and the other was a verifier-based authentication protocol. Lee et al. [8] proposed an improved encrypted key exchange protocol developed by Yeh's scheme. They claimed that the proposed protocols had the same computation complexity as Yeh's protocol. In [2] and [6], the server's public keys were both needed in their schemes. Lu and Cao [5] proposed a new simple three-party password-based authenticated key exchange protocol (S-3PAKE) which did not require any server's public key. Guo et al. [11] found that S-3PAKE in [5] was vulnerable to a kind of man-in-the-middle attack that exploited an authentication flaw in the

*Correspondence: jwliu@mail.xidian.edu.cn
Xidian University, Taibai South Road, 710071 Xi'an, China

protocol and is subject to the undetectable online dictionary attack. Then, they have provided an improved version. Kim and Choi [12] proposed another improved version of S-3PAKE against the online password guessing attack. However, both of the two improved versions in [11] and [12] had more computation cost than the original S-3PAKE protocol though they are more secure.

With efficiency and security in consideration, the number of protocol execution steps and the complexity of cryptographic operations have been used to measure the performance of the existing 3PAKE schemes. Different from the above existing 3PAKE protocols with less consideration of computation cost, Huang [7] proposed a 3PAKE protocol in five steps without improving the server's public key. In [1–3], the authors presented several symmetric key-based authenticated key exchange protocols, respectively. In order to further improve the efficiency of 3PAKE protocols, in this paper, we propose two new efficient three-party authenticated key exchange protocols with one-time key for WBANs especially, which achieve more security properties as Huang's scheme claimed.

WBAN is the embranchment of wireless sensor network, which can benefit to monitor and improve health conditions of people, surveillance of old age, and handicapped people [13]. It can further improve quality of life by monitoring and examining the vital signs (e.g., temperature, blood pressure, etc.) of healthy people to avoid future health problems. The study on wireless body area network is in a fledging period at present, meanwhile IEEE raised 802.15.6 standard for wireless body area network in 2012, which regulates the technical requirements in each layers of WBAN. WBANs include various types of medical and non-medical sensors equipped in and on human bodies to monitor different biological information of people. All BAN nodes send monitored data to a BAN controller. In WBANs, each BN with biosensors must be operated with extremely stringent constrains, especially implanted BAN nodes. So, simplicity is an important factor in devising a new protocol for WBANs. Design considerations for efficient key exchange protocols for WBANs are as follows:

- The proposed key agreement protocol should not require lots of energy and memory because sensor nodes are already resource constraints.
- It must suit the topology structure of wireless body area network.
- Communication messages should be of low redundancy rate and minimum message exchange between the nodes.

Possible attacks in wireless channel (such as replaying attack, eavesdropping attack, denial of service attack, Byzantine attack, etc.) have raised concerns of users and medical service providers. The detail security requirements of WBANs are introduced in [14] that is not altogether different from general WSNs.

Star topology is largely used in the WBANs, which is simple and easy to control. In this topology, it is possible to partition the sensor nodes according to their location: on the head; on the torso; and on the limbs [15]. However, it will impose higher energy costs for communications involving nodes that are distant from the BAN Network Controller. For these nodes, we could consider using relay nodes. Till date, there are very few security protocols [16–18] designed for this kind of network topology in WBANs.

In this paper, the main contributions of our work can be summarized as follows:

- We propose two novel three-party authenticated key exchange protocols between controller node and sensor nodes in different situations. Due to the calculation ability and the storage capacity of sensor nodes, new protocols are specially based on symmetric cryptography.
- The BAN logic formal verification tool has been employed in aid design of 3PAKE protocol for authentication and security verification.
- The quantified performance analysis on the proposed 3PAKE protocols is conducted.

The rest of this paper is structured as follows. Section 2 briefly introduces the network model of WBANs. In Section 3, two three-party key exchanged protocols are proposed in different application scenarios, namely normal situation and critical or special situation. Section 4 presents the formal demonstration by BAN logic and security analysis of the new protocols. The performance comparisons between proposed protocols and others are conducted in Section 5. Finally, conclusion is drawn in Section 6.

2 Network model of the wireless body area network

WBAN is a special branch of the wireless sensor network. It is a human body-centered communication network [19], consisting of body-related elements, including devices such as sensors distributed within and deployed around the human body. Through WBAN, people can transfer data of intracorporal sensors to the terminal equipments taken along, implement real-time health monitoring and auxiliary diagnosis of disease further for the patients [20], and meanwhile realize the network interconnection within the scope of human and so forth.

The 802.15.6 standard on WBAN gives out the topology model of such net, the two-hop star topology, composed by a hub node and several descendants, the number of which ranges from several to dozens. Here, except the hub, we differentiate the nodes as primary node and secondary node logically while the nodes have the same attribute. The affiliation of the nodes is shown in Fig. 1. The link hub-S_1-S_{11} means the two-hop connection between the hub and secondary node S_{11}, and hub-S_2-S_{21} means the two-hop connection between the hub and secondary node S_{21}.

Considering the net as a two-tier architecture, the control node (hub) is linked together with the primary sensor node S_1, $S_2 \cdots S_n$ logically so as to transmit data. Simultaneously, a portion of primary nodes S_i are connected with the corresponding secondary nodes S_{i1} in the second layer. Here, actually, the primary node plays the rule of relay node. In the initial condition, authentication process of each node should be conducted at the first place, before the session key is generated. It requires the adoption of authentication and key exchange protocol.

3 New authenticated key exchange protocols for wireless body area network

In this section, we give the description of two proposed protocols using two-hop star topology. The protocols are explained in two different application scenarios. For the sake of simplicity, we make *S* denote the control node and *B*, *C*, *D* represent the primary nodes respectively, with *A* representing a secondary node. In the initial state, the control node *S* keeps the pre-shared key K_{bs} with primary node *B*, and K_{cs} with *C*, also K_{ds} with *D*, *S* shares the pre-shared key K_{as} with secondary nodes *A* identically.

3.1 Formalizing description of protocol I

In normal cases, the normal nodes periodically collect data from sensor nodes in WBANs and then send these data to the hub. If secondary node is near enough to the hub, it can establish connection with the hub directly. If not, it has to find a primary node as a relay to complete the connection.

Protocol I begins with a message broadcasted by a secondary node *A*. After receiving the message from *A*, the adjacent node *B*, *C*, *D* generates encrypted message respectively according to the received message, then send it to the control node *S*. Subsequently, *S* determines which primary node is appropriate to be connected with node *A*. Assuming that *B* is the most appropriate one, the protocol will accomplish the authentication between *S* and *A*, *S* and *B*, as well as *A* and *B*, respectively, and generate a session key named *KEY* between *S* and *B*, session key K_{ab} between *A* and *B* correspondingly. At the same time, *S* replies to *C*, *D* to inform about the connection failure. Authentication flow diagram is shown in Fig. 2.

The formalizing description of protocol I:

Message1: A broadcast: A, Na
Message2: B$\longrightarrow$S: B, $\{$A, B, Na, Nb$\}_{K_{bs}}$
Message3: S$\longrightarrow$B: $\{$B, Na, $K_{ab}\}_{K_{as}}$, $\{$A, Nb, K_{ab}, KEY$\}_{K_{bs}}$
Message3': S$\longrightarrow$C: $\{$Nc, text$\}_{K_{cs}}$
Message4: B$\longrightarrow$A: $\{$B, Na, $K_{ab}\}_{K_{as}}$, $\{$Na, Nb$\}_{K_{ab}}$
Message5: A$\longrightarrow$B: $\{$Nb$\}_{K_{ab}}$

The analysis of the protocol I:

(1) The secondary node *A*, which is supposed to access to the network for authentication, broadcasts Message 1 including its own identifier *A* and generates a random number *Na*. After receiving the broadcasted message, *B*, *C*, *D* sends Message 2 to *S*.

(2) *B* sends a message encrypted with the pre-shared key K_{bs} to *S*, which contains identifier *A*, random *Na*, identifier *B*, and random number *Nb* generated by node *B*. Node *C*, *D* also sends the same type of messages.

(3) After receiving the request messages sent by primary nodes, *S* decrypts the messages by pre-shared key. Noticing that it is secondary node *A* that wants to be authenticated to join the network, *S* determines the most suitable primary node to be connected with *A* and sends Message 3 to the right node *B* as a reply, meanwhile *S* sends Message 3' to *C*, *D*. Message 3 involves $\{B, Na, K_{ab}\}$ encrypted with K_{as} and $\{A, Nb, K_{ab}, KEY\}$ encrypted with K_{bs}. Among them,

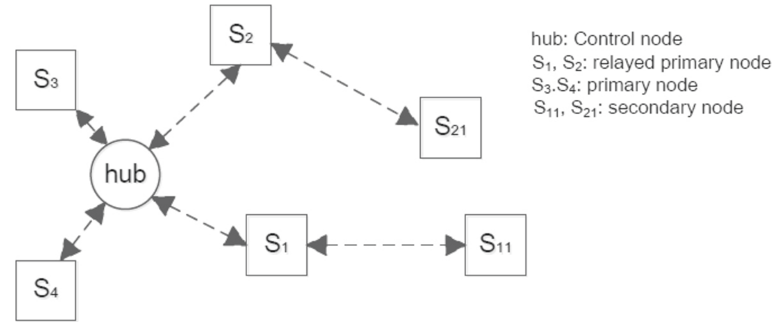

Fig. 1 The structure of two-hop star topology of wireless body area network

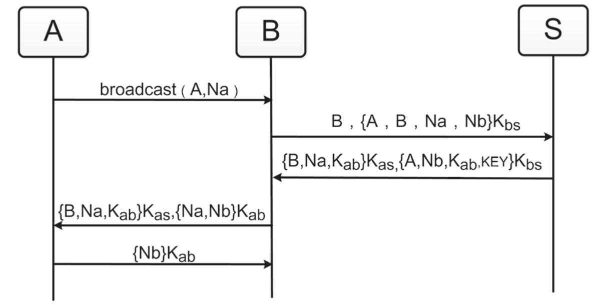
A
B
S
broadcast (A,Na)
B , {A , B , Na , Nb}K_{bs}
{B,Na,K_{ab}}K_{as},{A,Nb,K_{ab},KEY}K_{bs}
{B,Na,K_{ab}}K_{as},{Na,Nb}K_{ab}
{Nb}K_{ab}

Fig. 2 The flow chart of the certification process of protocol I

$\mathrm{K_{ab}}$ is the session key for *A* and *B* generated by *S*, and *KEY* is the session key between *B* and *S* generated by *S*.

(4) After receiving Message 3, *B* decrypts the message with $\mathrm{K_{bs}}$ and gets the session *KEY* and $\mathrm{K_{ab}}$ then encrypts the random number *Na*, *Nb* with $\mathrm{K_{ab}}$, together with $\{B, Na, \mathrm{K_{ab}}\}_{\mathrm{K_{as}}}$ and forwards them to node *A*. At the same time, node *C*, *D* receives the replied messages from *S* and knows that it is unable to connect with *A*.

(5) After receiving the previous message, *A* decrypts message $\{B, Na, \mathrm{K_{ab}}\}_{\mathrm{K_{as}}}$ with $\mathrm{K_{as}}$ firstly to obtain the session key $\mathrm{K_{ab}}$, then decrypts message $\{Na, Nb\}_{\mathrm{K_{ab}}}$ with $\mathrm{K_{ab}}$ to get two random numbers *Na* and *Nb*, and finally verifies whether they are same. If so, *A* sends *Nb* encrypted with $\mathrm{K_{ab}}$ to *B*, otherwise the authentication fails.

(6) After receiving the message from node *A*, node *B* tests whether the assumed *Nb* is identical with the original one, if so it shows that node *A* has received the correct session key, then end the protocol.

3.2 Formalizing description of protocol II

In some special cases, the primary node and the secondary node must work together to analyze the data collected from the human body, for example, measuring the blood circulation system. The primary node measures blood pressure, while the secondary node measures blood oxygen. Each primary node measuring blood pressure is connected to a secondary node measuring blood oxygen. That is to say, whenever a primary node broadcasts requirements, there must be a synergistic secondary node in response. The protocol II is proposed for this kind of special application cases.

The primary node *B* broadcasts a message first, and then the corresponding coordination secondary node *A* generates an encrypted message and sends it to the primary node *B* after receiving the broadcast message. On receiving message from node *A*, node *B* attaches its own information and encrypts all of them, then sends them to the control node *S*. *S* decrypts and certificates the received message. If the message is proved correctly, *S* sends the feedback information which contains the session keys to node *B*, such as $\mathrm{K_{AB}}$ between node *A* and node *B* and $\mathrm{K_{BS}}$ between node *S* and node *B*. Node *B* sends the message which includes $\mathrm{K_{AB}}$ to *A*, and *A* gives a reply to node *B* after receiving and confirming it correctly. Authentication flow chart is shown in Fig. 3.

The formalizing description of protocol II:

Message1: B broadcast: B, Nb
Message2: A⟶B: $A, Na, Nb, \{A, B, Na\}_{K_{as}}$
Message3: B⟶S: $B, \{\{A, Na, B\}_{K_{as}}, A, Nb\}_{K_{bs}}$
Message4: S⟶B: $\{A, Nb, K_{AB}, K_{BS}\}_{K_{bs}}, \{Na, B, K_{AB}\}_{K_{as}}$
Message5: B⟶A: $\{Na, B, K_{AB}\}_{K_{as}}, \{Nb\}_{K_{AB}}$
Message6: A⟶B: $\{Nb + 1\}_{K_{AB}}$

The analysis of the protocol II:

(1) The primary node *B* broadcasts its own identifier *B* and generates a random number *Nb*.

(2) The secondary node *A* which cooperates with node *B* sends a message, which contains plain text identifier *A*, random *Na*, *Nb*, identifier *B*, and identifier *A*, identifier *B*, random *Na* encrypted with the pre-shared key $\mathrm{K_{as}}$.

(3) After receiving the messages sent by secondary nodes *A*, *B* encrypts the encrypted message $\{A, B, Na\}_{K_{as}}$ and identifier *A*, random *Nb* with pre-shared key $\mathrm{K_{bs}}$, along with plain text identifier *B*, and sends them to the control node *S*.

(4) After receiving Message 3, *S* decrypts the message and verifies it. If correct, *S* generates the session key $\mathrm{K_{BS}}$ between *S* and *B*, and session key $\mathrm{K_{AB}}$, between *A* and *B*. *S* uses $\mathrm{K_{bs}}$ to encrypt *A*, *Nb*, $\mathrm{K_{AB}}$, and $\mathrm{K_{BS}}$ and uses $\mathrm{K_{as}}$ to encrypt *B*, *Na* and $\mathrm{K_{AB}}$, then send them to node *B*.

(5) After receiving the previous message and decrypting the first part, node *B* uses $\mathrm{K_{bs}}$ to get session key $\mathrm{K_{BS}}$

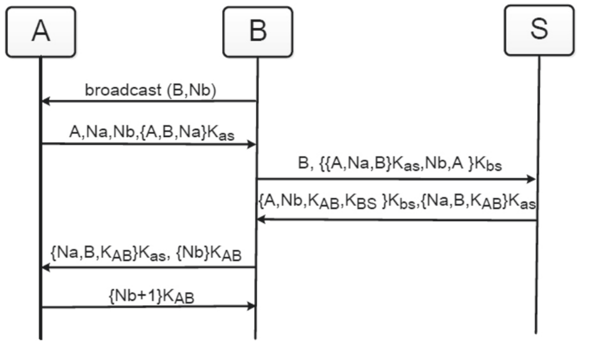
A
B
S
broadcast (B,Nb)
A,Na,Nb,{A,B,Na}K_{as}
B, {{A,Na,B}K_{as},Nb,A }K_{bs}
{A,Nb,K_{AB},K_{BS} }K_{bs},{Na,B,K_{AB}}K_{as}
{Na,B,K_{AB}}K_{as}, {Nb}K_{AB}
{Nb+1}K_{AB}

Fig. 3 The flow chart of the certification process of protocol II

and K_{AB}, uses K_{AB} to encrypt *Nb*, and sends node *A* the message $\{Na, B, K_{AB}\}_{K_{as}}$.

(6) After receiving the message from node *B*, *A* decrypts the front part of the message and uses K_{as} to get K_{AB}, random number and identifier, then verifies if the characteristic is right. If so, node *A* decrypts the second part and uses the new received session key K_{AB} to get *Nb*. If the received *Nb* is the same with original one generated by node *B*, *A* sends $Nb + 1$ encrypted with K_{AB} to node *B*.

(7) After receiving the message, node *B* decrypts it to get $Nb + 1$, then has $Nb + 1$ minus one, and checks if it is the same with the random *Nb* generated in the first step. If so, the protocol performs successfully, otherwise the authentication fails.

Primary and secondary nodes are synergistic, that is to say, the primary node sends messages to the control node *S* while the secondary node sends messages by virtue of primary nodes at the same time. After the protocol completes initialization and certification, the primary node *B* will send Message 2 to control node *S*, and secondary node *A* will send Message 1 to *S*. Simultaneously, node *A* encrypts Message 1 with session key K_{AB} and sends the original message to node *B*. *B* decrypts Message 1 with K_{AB} concatenate Message 2 and encrypts them with K_{BS} then sends the original message to *S*. Finally, *S* decrypts messages with K_{BS} and obtains Message 1 and Message 2.

4 Security analysis

Security analysis is an important way of detecting possible security flaws in security protocols. In this section, we give both the formalization analysis by BAN logic and non-formalization analysis of the proposed protocols.

4.1 Formal analysis

The two kinds of authenticated key exchange protocols are testified by the celebrated BAN logic in this subsection. The authentication logic is one of the most commonly used analysis tools of cryptographic protocols. BAN logic [21, 22] has not only revealed lots of flaws of famous protocols but also found the redundancy of many protocols. In BAN logic, messages are being idealized as formulas in the first place. After that, the initial state assumptions are defined as the case may be. Then, by making use of the known conditions and the logic regulations, it is reasonable to judge and to ratiocinate whether the protocols meet the goals or not.

4.1.1 Logical symbol

Below are logical symbols of BAN logic used in this paper:

1. P, Q: subjects, those are the principles participant in the protocol
2. X: message
3. K: secret key
4. $\{X\}_K$: message X is encrypted with K
5. $P|\equiv Q$: P believes Q
6. $P \lhd X$: P has received message X
7. $P| \sim X$: *P* said *X*
8. $Q \Rightarrow X$: Q has the jurisdiction to X
9. $\sharp(X)$: X is fresh
10. $P \overset{K}{\longleftrightarrow} Q$: K is the common pre-share key of P and Q

4.1.2 Inference rule

BAN logic contains message-meaning rules, nonce-verification rule, jurisdiction rules, and so forth. The messages above the horizontal line are known conditions while below line are the results deduced from the known conditions.

1. Message-meaning rules: *P* shares the secret key *K* with *Q*. If *P* receives a message *X* encrypted with *K*, then *P* believes that *Q* has sent *X*.

$$\mathrm{M1}: \frac{P| \equiv P \overset{K}{\longleftrightarrow} Q, P \lhd \{X\}_{K_X}}{P| \equiv Q| \sim X}$$

2. Nonce-verification rule: if *P* believes that message *X* is fresh and believes that *Q* has sent *X*, then *P* believes that *Q* believes *X*.

$$\mathrm{N1}: \frac{P| \equiv \sharp(X), P| \equiv Q| \sim X}{P| \equiv Q| \equiv X}$$

3. Jurisdiction rules: if *P* believes *Q* has sent message *X*, and *P* believes *Q* believes *X*, then *P* believes *X*.

$$\mathrm{J1}: \frac{P| \equiv Q \Rightarrow X, P| \equiv Q| \equiv X}{P| \equiv X}$$

4. Belief-joint rules: if *P* believes *X* and *Y*, then *P* believes messages of a cascade of *X* and *Y*; if *P* believes that *Q* believes messages of a cascade of *X* and *Y*, then *P* believes *Q* believes *X* or *Y*; if *P* believes that *Q* has said *X* and *Y*, then *P* believes *Q* has said *X* or *Y*; if *P* believes the message of a cascade of *X* and *Y*, then *P* believes *X* or *Y*.

$$\mathrm{B1}: \frac{P| \equiv X, P| \equiv Y}{P| \equiv (X, Y)} \qquad \mathrm{B2}: \frac{P| \equiv Q| \equiv (X, Y)}{P| \equiv Q| \equiv Y}$$

$$\mathrm{B3}: \frac{P| \equiv Q| \sim (X, Y)}{P| \equiv Q| \sim X} \qquad \mathrm{B4}: \frac{P| \equiv (X, Y)}{P| \equiv X}$$

5. Freshness-joint rule: if *P* believes that *X* is fresh, *P* believes the entire message that cascade with *X* is fresh.

$$\mathrm{F1}: \frac{P| \equiv \sharp(X)}{P| \equiv \sharp(X, Y)}$$

6. Reception rules: if *P* receives messages of a cascade of *X* and *Y*, we consider *P* receives *X* or *Y*; if *P* receives the connection of formula of *X* and *Y*, we consider *P*

receives X or Y; P shares secret key K with Q. If P receives message X encrypted with K, we can infer that P receives X.

$$\mathrm{R1}: \frac{P \lhd (X,Y)}{P \lhd X} \qquad \mathrm{R2}: \frac{P\lhd < X >_Y}{P \lhd X}$$

$$\mathrm{R3}: \frac{P| \equiv P \xleftrightarrow{K} Q, P \lhd \{X\}_K}{P \lhd X}$$

7. Additional rules: secret key K is fresh. If P receives message X encrypted with K and P believes P shares secret key K with Q, we can infer that P believes Q has sent message X, and P believes Q believes P shares secret key K with Q.

$$\frac{\sharp(K), P \lhd \{X\}_K, P| \equiv P \xleftrightarrow{K} Q}{P| \equiv P| \sim X, P| \equiv Q| \equiv P \xleftrightarrow{K} Q}$$

4.1.3 The deduction of protocol I

(1) Idealization

- $MS2 : B \rightarrow S,\ B, \{A,B,Na,Nb\}_{K_{bs}}$
- $MS3 : S \rightarrow B, \{Na,B,K_{ab}\}_{K_{as}}, \{A,Nb,Kab,KEY\}_{K_{bs}}$
- $MS4 : B \rightarrow A, \{B,Na,K_{ab}\}_{K_{as}}, \{Na,Nb\}_{K_{ab}}$
- $MS5 : A \rightarrow B, \{Nb\}_{K_{ab}}$

The idealization of messages1 is omitted since it does not contribute to the logical properties of the protocol.

(2) Initial state assumptions

The initial state assumptions of S are:

1. $S| \equiv S \xleftrightarrow{K_{as}} A$
2. $S| \equiv S \xleftrightarrow{K_{bs}} B$
3. $S \Rightarrow KEY$
4. $S \Rightarrow K_{ab}$

The initial state assumptions of B are:

1. $B| \equiv B \xleftrightarrow{K_{bs}} S$
2. $S| \equiv \sharp(Nb)$
3. $B| \equiv S| \Rightarrow B \xleftrightarrow{KEY} S$
4. $B| \equiv S| \Rightarrow A \xleftrightarrow{K_{ab}} B$

The initial state assumptions of A are:

1. $A| \equiv A \xleftrightarrow{K_{as}} S$
2. $A| \equiv S| \Rightarrow A \xleftrightarrow{K_{ab}} B$
3. $A| \equiv \sharp(Na)$

(3) Annotation

1 $\mathrm{S}\lhd\{\mathrm{A,B,Na,Nb}\}_{\mathrm{K_{bs}}}$

2 $\mathrm{B}\lhd \left\{\mathrm{Na, A} \xleftrightarrow{\mathrm{K_{ab}}} \mathrm{B}, \sharp \left(\mathrm{A} \xleftrightarrow{\mathrm{K_{ab}}} \mathrm{B}\right)\right\}_{\mathrm{K_{as}}},$
$\left\{\mathrm{Nb, A} \xleftrightarrow{\mathrm{K_{ab}}} \mathrm{B}, \sharp \left(\mathrm{A} \xleftrightarrow{\mathrm{K_{ab}}} \mathrm{B}\right), \mathrm{S} \xleftrightarrow{\mathrm{KEY}} \mathrm{B}, \sharp \left(\mathrm{S} \xleftrightarrow{\mathrm{KEY}} \mathrm{B}\right)\right\}_{\mathrm{K_{bs}}}$

3 $\mathrm{A}\lhd \left\{\mathrm{Na, A} \xleftrightarrow{\mathrm{K_{ab}}} \mathrm{B}, \sharp \left(\mathrm{A} \xleftrightarrow{\mathrm{K_{ab}}} \mathrm{B}\right)\right\}_{\mathrm{K_{as}}},$
$\left\{\mathrm{Na, Nb, A} \xleftrightarrow{\mathrm{K_{ab}}} \mathrm{B}\right\}_{\mathrm{K_{ab}}}$

4 $\mathrm{B}\lhd \left\{\mathrm{Nb, A} \xleftrightarrow{\mathrm{K_{ab}}} \mathrm{B}\right\}_{\mathrm{K_{ab}}}$

(4) Final faith After the protocol runs successfully, it should achieve the following certification targets.

- S and B realize two-way authentication
  $S| \equiv B| \sim X_B$
  $B| \equiv S| \sim X_S$ (X_S and X_B are the messages generated by S and B)
- B and A realize two-way authentication
  $B| \equiv A| \sim X_A$
  $A| \equiv B| \sim X_B$ (X_A and X_B are the messages generated by A and B)
- Using two-way authentication to negotiate shared secret key
  $B| \equiv B \xleftrightarrow{KEY} S$ $\qquad B| \equiv S| \equiv B \xleftrightarrow{KEY}$
  S
  $B| \equiv B \xleftrightarrow{K_{ab}} A$ $\qquad B| \equiv A| \equiv B \xleftrightarrow{K_{ab}}$
  A
  $A| \equiv A \xleftrightarrow{K_{ab}} S$ $\qquad A| \equiv B| \equiv A \xleftrightarrow{K_{ab}}$
  B

(5) Derivation process

According to MS2:

1 $\dfrac{S|\equiv S\xleftrightarrow{K_{bs}}B,S\lhd\{A,B,Na,Nb\}_{K_{bs}}}{S|\equiv B|\sim\{A,B,Na,Nb\}}$ $\qquad (M1)$

According to MS3:

1. $\dfrac{B|\equiv B\xleftrightarrow{K_{bs}}S,B\lhd\{A,Nb,K_{ab},KEY\}_{K_{bs}}}{B|\equiv S|\sim\{A,Nb,K_{ab},KEY\}}$ $\qquad (M1)$
2. $\dfrac{B|\equiv S|\sim\{A,Nb,K_{ab},KEY\}}{B|\equiv S|\sim(KEY)}$ $\qquad (B3)$
3. $\dfrac{B|\equiv S|\sim(KEY),B|\equiv S|\Rightarrow KEY}{B|\equiv KEY}$ $\qquad (J)$
4. $\dfrac{B|\equiv S|\sim\{A,Nb,K_{ab},KEY\}}{B|\equiv S|\sim(K_{ab})}$ $\qquad (B3)$
5. $\dfrac{B|\equiv S|\sim(K_{ab}),B|\equiv S|\Rightarrow K_{ab}}{B|\equiv K_{ab}}$ $\qquad (J)$
6. $\dfrac{B|\equiv\sharp(Nb)}{B|\equiv\sharp\{A,Nb,K_{ab},KEY\}}$ $\qquad (F1)$
7. $\dfrac{B|\equiv S|\sim\{A,Nb,K_{ab},KEY\},B|\equiv\sharp\{A,Nb,K_{ab},KEY\}}{B|\equiv S|\equiv\{A,Nb,K_{ab},KEY\}}$ $\qquad (N1)$
8. $\dfrac{B|\equiv S|\equiv\{A,Nb,K_{ab},KEY\}}{B|\equiv S|\equiv KEY}$ $\qquad (B2)$

According to MS5:

1. $\frac{\sharp K_{ab}, B\lhd(Nb)_{K_{ab}}, B|\equiv K_{ab}}{B|\equiv A\sim(Nb), B|\equiv A|\equiv K_{ab}}$

According to MS4:

1. $\frac{A|\equiv A\xleftrightarrow{K_{as}}S, A\lhd\{B,Na,K_{ab}\}_{K_{as}}}{A|\equiv S|\sim\{B,Na,K_{ab}\}}$ $(M1)$
2. $\frac{A|\equiv\sharp(Na)}{A|\equiv\sharp\{Na,B,K_{ab}\}}$ $(F1)$
3. $\frac{A|\equiv\sharp\{Na,B,K_{ab}\}, A|\equiv S|\sim\{B,Na,K_{ab}\}}{A|\equiv S|\equiv\{B,Na,K_{ab}\}}$ $(N1)$
4. $\frac{A|\equiv S|\equiv\{B,Na,K_{ab}\}}{A|\equiv S|\equiv\{K_{ab}\}}$ $(B2)$
5. $\frac{A|\equiv S|\equiv\{K_{ab}\}, A|\equiv S|\Rightarrow\{K_{ab}\}}{A|\equiv\{K_{ab}\}}$ (J)
6. $\frac{\sharp K_{ab}, A|\equiv A\xleftrightarrow{K_{ab}}S, A\lhd\{Na,Nb\}_{K_{ab}}}{A|\equiv B|\sim\{Na,Nb\}, A|\equiv B|\equiv A\xleftrightarrow{K_{ab}}S}$

From the above derivation, we can draw the following conclusions: *B* has the *KEY* and believes that it is shared with *S*; *B* has the K_{ab} and believes that it is shared with *A*; *A* has the K_{ab} and believes that it is shared with *B*; *S* and *B* realize two-way authentication; *B* and *A* realize two-way authentication.

4.1.4 The deduction of protocol II

(1) Idealization

- $MS2: A\rightarrow B, \{A,B,Na\}_{K_{as}},\ A,\ Na,\ Nb$
- $MS3: B\rightarrow S,\ B, \{\{A,Na,B\}_{K_{as}}, Nb, A\}_{K_{bs}}$
- $MS4: S\rightarrow B, \{A,Nb,K_{AB},K_{BS}\}_{K_{bs}}, \{Na,B,K_{AB}\}_{K_{as}}$
- $MS5: B\rightarrow A, \{Na,B,K_{AB}\}_{K_{as}}, \{Nb\}_{K_{AB}}$
- $MS6: A\rightarrow B, \{Nb+1\}_{K_{AB}}$

The idealization of Message 1 and part of Message 2 are omitted since it does not contribute to the logical properties of the protocol.

(2) Initial state assumptions

The initial state assumptions of *S* are:

1. $S|\equiv S\xleftrightarrow{K_{as}}A$
2. $S|\equiv S\xleftrightarrow{K_{bs}}B$
3. $S\Rightarrow K_{BS}$
4. $S\Rightarrow K_{AB}$

The initial state assumptions of *B* are:

1. $B|\equiv B\xleftrightarrow{K_{bs}}S$
2. $S|\equiv\sharp(Nb)$
3. $B|\equiv S|\Rightarrow B\xleftrightarrow{K_{BS}}S$
4. $B|\equiv S|\Rightarrow A\xleftrightarrow{K_{AB}}B$

The initial state assumptions of *A* are:

1. $A|\equiv A\xleftrightarrow{K_{as}}S$
2. $A|\equiv S|\Rightarrow A\xleftrightarrow{K_{AB}}B$
3. $A|\equiv\sharp(Na)$

(3) Annotation

1: $\mathrm{B}\lhd\{\mathrm{A,B,Na}\}_{\mathrm{K_{as}}}$
2: $\mathrm{S}\lhd\{\{\mathrm{A,Na,B}\}_{K_{as}},\mathrm{A,B,Nb}\}_{K_{bs}}$
3: $\mathrm{B}\lhd\ \{\mathrm{Nb,A}\xleftrightarrow{\mathrm{K_{AB}}}\mathrm{B},\sharp(\mathrm{A}\xleftrightarrow{\mathrm{K_{AB}}}\mathrm{B}),\mathrm{B}\xleftrightarrow{\mathrm{K_{BS}}}\mathrm{S},\sharp(\mathrm{B}\xleftrightarrow{\mathrm{K_{BS}}}\mathrm{S})\}_{\mathrm{K_{bs}}}, \{\mathrm{Na,A}\xleftrightarrow{\mathrm{K_{AB}}}\mathrm{B},\sharp(\mathrm{A}\xleftrightarrow{\mathrm{K_{AB}}}\mathrm{B})\}_{\mathrm{K_{as}}}$
4: $\mathrm{A}\lhd\ \{\mathrm{Na,A}\xleftrightarrow{\mathrm{K_{AB}}}\mathrm{B},\sharp(\mathrm{A}\xleftrightarrow{\mathrm{K_{AB}}}\mathrm{B})\}_{\mathrm{K_{as}}},\{\mathrm{Nb}\}_{\mathrm{K_{AB}}}$
5: $\mathrm{B}\lhd\{\mathrm{Nb+1}\}_{K_{AB}}$

(4) Final faith

After the protocol runs successfully, it should achieve the following certification targets.

- *S* and *B* realize two-way authentication
  $S|\equiv B|\sim X_B$
  $B|\equiv S|\sim X_S$ (X_S and X_B are the messages generated by *S* and *B*)
- *B* and *A* realize two-way authentication
  $B|\equiv A|\sim X_A$
  $A|\equiv B|\sim X_B$ (X_A and X_B are the messages generated by *A* and *B*)
- Using two-way authentication to negotiate shared secret key
  $B|\equiv B\xleftrightarrow{K_{BS}}S$ $B|\equiv S|\equiv B\xleftrightarrow{K_{BS}}$
  S
  $B|\equiv B\xleftrightarrow{K_{AB}}A$ $B|\equiv A|\equiv B\xleftrightarrow{K_{AB}}$
  A
  $A|\equiv A\xleftrightarrow{K_{AB}}S$ $A|\equiv B|\equiv A\xleftrightarrow{K_{AB}}$
  B

(5) Derivation process

According to MS3:

1. $\frac{S|\equiv S\xleftrightarrow{K_{bs}}B, S\lhd\{\{A,Na,B\}_{K_{as}},Nb,A\}_{K_{bs}}}{S|\equiv B|\sim\{\{A,Na,B\}_{K_{as}},Nb,A\}}$ $(M1)$

According to MS4:

1. $\frac{B|\equiv B\xleftrightarrow{K_{bs}}S, B\lhd\{A,Nb,K_{AB},K_{BS}\}_{K_{bs}}}{B|\equiv S|\sim\{A,Nb,K_{AB},K_{BS}\}}$ $(M1)$
2. $\frac{B|\equiv S|\sim\{A,Nb,K_{AB},K_{BS}\}}{B|\equiv S|\sim(K_{BS})}$ $(B3)$
3. $\frac{B|\equiv S|\sim(K_{BS}), B|\equiv S|\equiv\Rightarrow KEY}{B|\equiv K_{BS}}$ (J)
4. $\frac{B|\equiv S|\sim\{A,Nb,K_{AB},K_{BS}\}}{B|\equiv S|\sim(K_{AB})}$ $(B3)$
5. $\frac{B|\equiv S|\sim(K_{AB}), B|\equiv S|\Rightarrow K_{AB}}{B|\equiv K_{AB}}$ (J)
6. $\frac{B|\equiv\sharp(Nb)}{B|\equiv\sharp\{Nb,A,K_{AB},K_{BS}\}}$ $(F1)$
7. $\frac{B|\equiv S|\sim\{A,Nb,K_{AB},K_{BS}\}, B|\equiv\sharp\{A,Nb,K_{AB},K_{BS}\}}{B|\equiv S|\equiv\{A,Nb,K_{AB},K_{BS}\}}$ $(N1)$

8. $\frac{B|\equiv S|\equiv\{A,Nb,K_{AB},K_{BS}\}}{B|\equiv S|\equiv K_{BS}}$ $(B2)$

According to MS6:

1. $\frac{\sharp K_{ab},B\lhd(Nb+1)_{K_{AB}},B|\equiv K_{AB}}{B|\equiv A\sim(Nb+1),B|\equiv A|\equiv K_{AB}}$

According to MS5:

1. $\frac{A|\equiv A\overset{K_{as}}{\longleftrightarrow}S,A\lhd\{Na,B,K_{AB}\}_{K_{as}}}{A|\equiv S|\sim\{B,Na,K_{AB}\}}$ $(M1)$

2. $\frac{A|\equiv\sharp(Na)}{A|\equiv\sharp\{Na,B,K_{AB}\}}$ $(F1)$

3. $\frac{A|\equiv S|\sim\{B,Na,K_{AB}\},A|\equiv\sharp\{Na,B,K_{AB}\}}{A|\equiv S|\equiv\{B,Na,K_{AB}\}}$ $(N1)$

4. $\frac{A|\equiv S|\equiv\{B,Na,K_{AB}\}}{A|\equiv S|\equiv\{K_{AB}\}}$ $(B2)$

5. $\frac{A|\equiv S|\equiv\{K_{AB}\},A|\equiv S|\Rightarrow\{K_{AB}\}}{A|\equiv\{K_{AB}\}}$ (J)

6. $\frac{\sharp K_{AB},A\lhd\{Nb\}_{K_{AB}},A|\equiv A\overset{K_{AB}}{\longleftrightarrow}S}{A|\equiv B|\sim\{Nb\},A|\equiv B|\equiv A\overset{K_{AB}}{\longleftrightarrow}S}$

From the above derivation, we can draw the following conclusions: B has the K_{BS} and believes that it is shared with S; B has the K_{AB} and believes that it is shared with A; A has the K_{AB} and believes that it is shared with B; S and B realize two-way authentication; B and A realize two-way authentication.

4.2 Security properties analysis

Firstly, the proposed protocols have the following properties.

Mutual authentication: By our protocols, S can authenticate A and B respectively from the authentication request with the random number Na and Nb. Also, A and B authenticate each other identity through K_{ab} and Nb. The protocols have mutual authentication property to make the man-in-the-middle attacks necessarily unsuccessful.

Perfect forward secrecy: Our protocols possess forward secrecy. An agreed key will not be compromised even if the other agreed keys derived from the same long-term keying material in a subsequent run are compromised. By the proposed protocols, the session key K_{ab} and KEY are randomly selected, so they are independent among each protocol execution. Therefore, the compromised keys K_{as} and K_{bs} cannot reveal any previous session keys.

Then, we analyze the proposed protocols under the following kinds of attacks.

Trivial substitution and replay attack: Replaying attack means that an adversary first intercepts some communication data in the currently running of key exchange protocol run. Then, he replays the intercepted data with receiver in a future protocol running. The replay attack does not succeed in the proposed protocols because the freshness of messages transmitted between participants are guaranteed by the random nonces Na and Nb. Only A, B, and S can use the pre-shared key to encrypt the random nonces. Moreover, the proposed protocols do not require the time-stamp information to prevent replay attack which requires extremely imperative precise clock synchronization.

Man-in-the-middle attack: A man-in-the-middle attack means that an attacker can intercept, replay, substitute, or modify the information that is significant to the communication parties. Since all critical messages in the proposed protocols are encrypted to prevent eavesdropping, it is rarely able to modify the messages exchanged between entities. However, if an attacker I eavesdrops the communication channel between A and B, he can replace the authentication request {Na, A} with {Ni, I}. The replaced {Ni, I} will be forward to the S together with {Nb, B}. The attacker can be successfully authenticated by S if he is really a legitimate user in the system. However, the man-in-the-middle attack can still not be successful because the attacker cannot generate a correct $\{Ni\}_{K_{ab}}$ to respond to the {Ni, I}. Therefore, we conclude that a man-in-the-middle attack could not succeed against the proposed protocols.

Fake base station attack: False base station attack is that a fake node pretends to be a participant node in the protocol, to grasp the secret information. For pre-shared key is only known between A, B, and S in the new protocols, the transmitted information encrypted by the pre-shared secret key K_{as} and K_{bs} will not be decrypted by illegal entities. The fake entities do not know the pre-shared key, thereby it cannot get the resulting session key eventually. If the entities decrypt the messages correctly and obtain the right contents, we can make sure that the identities of the nodes are legal. Then, the authentication is accomplished.

5 The performance analysis of the protocols

In this paper, we propose two efficient key exchange protocols under normal conditions and special conditions, respectively. From the performance perspective, we mainly concern the computational time and energy consumption of our protocols. To detail the quantitative result, we conduct simulations and compare our protocols with several typical protocols. Firstly, we make detail analysis of the computation time which is vital to the efficiency of the protocols. Then, we conclude a discussion of energy consumption on computation.

5.1 Computation time

In this section, we analyze and test the computation time associated with the efficiency of protocols.

Simulation environment setup: In this part, we setup a simulation hardware environment to measure the computation time of the selected schemes. The simulation environment is a 32-bit Cortex-M3 microcontroller with 72MHz ARM MCU and 512 KB memory. For each protocol, AES is selected as the secret key encryption scheme and SHA256 for hash function. The random number is generated with three times AES-128 cryptographic algorithm and two times XOR operations. The simulations are run several times to eliminate the randomness.

Simulation results: Noting that the computation overhead of these schemes mainly results from the cryptographic operations, thus the computation time consumed on the cryptographic operations can be used to approximate the efficiency of the schemes for the sake of simplicity. Table 1 shows the operating time of each algorithm. Given the cryptographic operations and their corresponding consuming time, we can calculate the computation time of each protocol as shown in Table 2. The corresponding figure is shown in Fig. 4.

From the simulations, we can find that the modular computations still cost much. It is clear that a good design of authenticated key exchange protocols should adopt suitable cryptographic operations with less computation in order to achieve better performance and efficiency. By comparing with other schemes, the proposed protocols show a relatively short time among all six schemes. In other four schemes, the computation time of relay node are time-consuming and will shorten the lifetime of the relay nodes which are not suited for WBAN environment. Therefore, this feature makes our protocols more effective. Based on these analyses, our schemes show a better performance in WBAN scenario.

5.2 Energy consumption

In this part, the energy consumption consumed by cryptographic operations is used to evaluate the schemes. This time, we use a low-processor and 64 MB memory running Windows Mobile 5.0 for packet pc. According to PXA270 [23], the typical power consumption of PXA270 in active is 570 mW. Therefore, using the computation time in Table 3, we can calculate the corresponding energy consumption. For example, if it takes 0.919 ms to complete a AES-128, the energy consumption is approximately $0.919 * 570/1000 = 0.523$ mJ. Similarly, based on Table 2, the energy consumption of all schemes is calculated as shown in Table 3. The corresponding figures are shown in Fig. 5.

Table 1 Computational time

Operations	Time(ms)
Secret key encrypt(AES-128)	0.919
Secret key decrypt(AES-128)	1.074
Random number	2.781
Hash	0.054
Modular	5.542

Table 2 Different schemes' computational time

Protocols	*A* (ms)	*B* (ms)	*S* (ms)
Lu [5]	19.569	19.569	36.141
Yoon [24]	23.377	23.377	27.266
Huang [7]	14.027	14.027	13.973
Lv [25]	16.831	20.686	16.885
Protocol I	9.07	15.968	9.655
Protocol II	9.834	14.894	10.729

Due to the computation energy consumption being proportional to the computational time, we can draw the same conclusions as the ones in Section 5.1.

5.3 Memory requirement of the protocols

In the protocols, a 2-byte-long node identifier is used to identify each node in the network, which starts from 0001 and increases on a sequential basis. In Table 4, we can find that the length of the random numbers generated by the nodes is 16 bytes, while pre-shared key K_{as}, K_{bs} and session key KEY, K_{ab}, K_{AB} and K_{BS} are all 16 bytes long. In the running process of the protocols, each node only needs to store the node identifier and the relevant random numbers, while the control node needs to generate and store the session keys additionally. The overall memory cost is no more than 1 KB. The ROM requirement of ordinary nodes including its identifier and pre-shared key is no more than 0.145 KB, and the memory requirement of RAM including random number and session key is no more than 0.25 KB. The ROM requirement of the control node including the pre-shared keys is at most 0.125 KB, and the RAM requirement including two pairs of the session key is no more than 0.25 KB. In summary, the overall

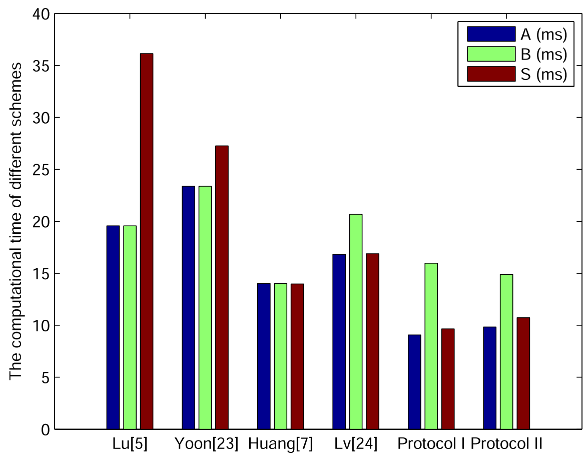

Fig. 4 The computational time of different schemes

Table 3 Different schemes' computational energy consumption

Protocols	*A* (mJ)	*B* (mJ)	*S* (mJ)
Lu [5]	11.154	11.154	20.600
Yoon [24]	13.324	13.324	7.594
Huang [7]	7.995	7.995	7.964
Lv [25]	9.593	11.791	9.624
Protocol I	5.169	9.101	5.503
Protocol II	5.605	8.489	6.115

memory requirement is quite small, which conforms to the limited capacity of WBAN nodes.

- The proposed protocol I : the total message size of the scheme is equal to $|A+Na|+|B|+|E_{bs}\{A+B+Na+Nb\}|+|E_{as}\{B+Na+K_{ab}\}|+|E_{bs}\{A+Nb+K_{ab}+KEY\}|+|E_{as}\{B+Na+K_{ab}\}|+|K_{ab}\{Na+Nb\}|+|E_{ab}\{Nb\}|$ Here, $|*|$ denotes the size of $'*'$ in byte. $E_c(*)$ represents the AES encryption algorithm calculated for the contents inside the bracket with c. The total message size of protocol I is 274 bytes.
- The proposed protocol II : the total message size of the scheme is equal to $|B+Nb|+|A+Nb+Na|+|E_{as}\{A+B+Na\}|+|B|+|E_{bs}\{E_{as}\{A+Na+B\}+Nb+A\}|+|E_{bs}\{A+Nb+K_{AB}+K_{BS}\}|+|E_{as}\{Na+B+K_{AB}\}|+|E_{as}\{Na+B+K_{AB}\}|+|E_{AB}\{Nb\}|+|E_{AB}\{Nb+1\}|$. The total message size is 422 bytes.

In the implementation procedure of authentication and session key generation of the authenticated key exchange protocols, the communication traffic is constant. That is to say, the length of messages is consistent. In protocol I and protocol II, the maximum communication traffic is no more than 0.5 KB. Communication traffic of the two protocols is extremely small, so the efficiency is higher.

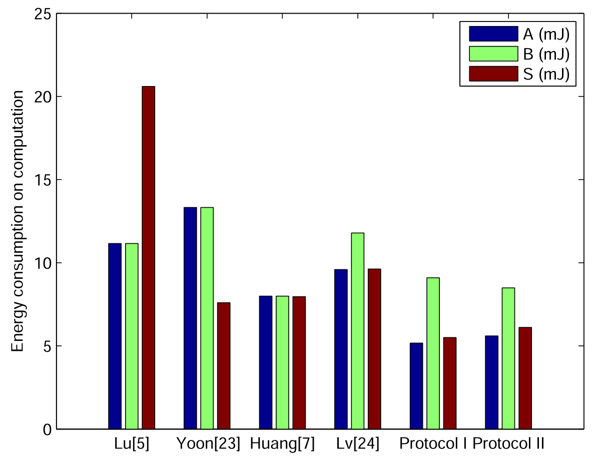

Fig. 5 Energy consumption on computation

Table 4 ROM requirement for keys

	ROM (byte)
Identify (A, B)	2
Random number (Na, Nb)	16
Pre-shared key (K_{as}, K_{bs})	16
Session key $(KEY, K_{ab}, K_{AB}, K_{BS})$	16

6 Conclusions

In this paper, we propose two authenticated key exchange protocols that are suitable for WBANs. The two schemes are proved to be secure in BAN logic model. The performance analysis of them are also given. The analysis results show that the proposed protocols achieve the expectative goals and possess several advantages: they provide favorable security performance and are capable of resisting sundry common attacks to guarantee communication security; the participants accomplish authentication and generate session key by five or six steps without tanglesome cryptographic operation; on account of majority security protocols utilizing timestamp to guarantee the freshness of messages, the participants must keep clock synchronization which is rather untoward and costly. However, the proposed protocols adopt random number instead of timestamp, reducing the complexity of the network as well as decreasing the cost. The performance analysis shows that the protocols have superior running time performance, less memory costs, and so forth. How to design more and better protocols for WBANs is the next target of further research.

Competing interests

The authors declare that they have no competing interests.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (No. 61100232), National Science and Technology Major Project of the Ministry of Science and Technology of China (No. 2013ZX03005007), the Fundamental Research Funds for the Central Universities (No. K5051301012), the 111 Project (B08038).

Received: 5 September 2014 Accepted: 1 June 2015
Published online: 03 July 2015

References

1. J Liao, B Zhu, Y He, Security analysis of NSSK protocol and its improvement. IEEE Int. Conf, 115–118 (2009). doi:10.1109/DASC.2009.44
2. Li, Shi L MX, in *3rd IEEE Conference on Industrial Electronics and Applications*. Security analysis and improvement of Yahalom protocol, (2008), pp. 1137-40
3. YJ Deng, Based on BAN logic analysis Otway-Rees protocol[J]. Chaohu Coll. J. **78**(3), 36–37 (2006)
4. HT Yeh, HM Sun, T Hwang, Efficient three-party authentication and key agreement protocols resistant to password guessing attacks. J. Inform. Sci. Eng. **19**(6), 1059–1070 (2003)

5. R Lu, Z Cao, Simple three-party key exchange protocol. Comput. Secur. **26**(1), 94–97 (2007)
6. T Chen, WB Lee, HB Chen, A round and computation-efficient three-party authenticated key exchange protocol. J. Syst. Softw. **81**(9), 1581–1590 (2008)
7. HF Huang, A simple three-party password-based key exchange protocol. Int. J. Commun. Syst. **22**(7), 857–862 (2009)
8. TF Lee, JL Liu, MJ Sung, SB Yang, CM Chen, Communication-efficient three-party protocols for authentication and key agreement. Comput. Math. Appl. **58**(4), 641–648 (2009)
9. X Li, JW Niu, S Kumari, MK Khan, J Liao, W Liang, Design and analysis of a chaotic maps-based three-party authenticated key agreement protocol. Nonlinear Dyn. **80** (2015). doi:10.1007/s11071-015-1937-0 in press
10. X Li, J Niu, MK Khan, JG Liao, An enhanced smart card based remote user password authentication scheme. J. Netw. Comp. Appl. 365, 1365–1371 (2013)
11. H Guo, Z Li, Y Mu, X Zhang, Cryptanalysis of simple three-party key exchange protocol. Comput. Secur. **27**(1-2), 16–21 (2008)
12. HS Kim, JY Choi, Enhanced password-based simple three-party key exchange protocol.Comput. Electrical Eng. **35**(1), 107–114 (2009)
13. HB Li, T Ken-ichi, B Zhen, K Ryuji, Body area network and its standardization at IEEE 802.15.MBAN. Mob. Wirel. Commun. Summit. **16th IST**, 1–5 (2007)
14. B Zhen, P Maulin, L SungHyup, W EunTae, A Arthur, TG6 technical Requirements Document (TRD). IEEE (2008). ID: 802.15-08-0644
15. W Burleson, SS Clark, B Ransford, K Fu, in *Proceedings of Design Automation Conference(DAC), 49th ACM/EDAC/IEEE*. Design challenges for secure implantable medical devices (IEEE, 2012), pp. 12–17
16. JM Ho, in *The 8th International Wireless Communications and Mobile Computing Conference (IWCMC)*. A versatile suite of strong authenticated key agreement protocols for body area networks (IEEE, Limassol, 2012), pp. 683–688. doi:10.1109/IWCMC.2012.6314287
17. SD Bao, YT Zhang, LF Shen, in *Proceeding of Wearable and Implantable Body Sensor Networks*. A design proposal of security architecture for medical body sensor networks (IEEE, BSN, 2006), pp. 84–90. doi:10.1109/BSN.2006.2
18. JW Liu, ZH Zhang, XF Chen, K Sup Kwak, Certificateless remote anonymous authentication schemes for wireless body area networks. IEEE Trans. Parallel Distributed Syst. **25**(2), 332–342 (2014)
19. B Latré, B Braem, I Moerman, A survey on wireless body area networks. J. Wireless Netw. **17**(1), 1–18 (2011)
20. M Rostami, W Burleson, A Juels, in *Design Automation Conference (DAC)*. Balancing security and utility in medical devices? (IEEE, 2013), pp. 1-6. 50th ACM/EDAC/IEEE
21. M Burrows, M Abadi, R Needham, *A logic of authentication.In:William Stallings*. (IEEE Computer Society Press, Practical Cryp tography for Data Internetworks, 1996)
22. JH Wen, M Zhang, X Li, The study on the application of BAN logic in formal analysis of authentication protocols. ACM Int. Conf. Proc. Series. **113**, 744-747 (2005). 7th International Conference on Electronic Commerce, ICEC05: Towards Ubiquitous Business
23. PXA270 processor electrical, mechanical, and thermal specification. http://pdf.dzsc.com/CXX/NHPXA270Cxxx.pdf
24. EJ Yoon, KY Yoo, Improving the novel three-party encrypted key exchange protocol. Comput. Stand. Interfaces. **30**(5), 309–314 (2008)
25. C Lv, M Ma, H Li, J Ma, An efficient three-party authenticated key exchange protocol with one-time key. IEEE INFOCOM, 1-5 (2010). doi:10.1109/INFCOMW.2010.5466648