J Med Syst (2019) 43: 19
https://doi.org/10.1007/s10916-018-1129-9

SYSTEMS-LEVEL QUALITY IMPROVEMENT

Analysis and Improvement of a Mutual Authentication Scheme for Wireless Body Area Networks

Rui Chen[1] · **Dezhong Peng**[2,3]

Received: 31 January 2018 / Accepted: 26 November 2018 / Published online: 18 December 2018

Abstract

An increase in aging population and the consequent chronic diseases pose not only serious effects to the economy but also a heavy burden to the medical system. Wireless body area networks (WBANs) provide a simple and low-cost strategy for health monitoring and telemedicine of the elderly. Many authentication schemes based on WBAN have been presented to address the sensitivity and privacy of collected data and the open characteristic of wireless networks. Wu et al. recently presented an efficient anonymous authentication scheme for WBANs, in which a one-side bilinear pairing methodology was applied to reduce the burden on the WBAN client side. However, we demonstrate that their scheme suffers from client impersonation attacks and that the adversary can easily forge a legal client to access the network service. In this paper, we analyze the limitations of Wu et al.'s scheme and design a novel mutual authentication scheme for WBANs that adopt asymmetric bilinear pairing to enhance security. Results of security and performance analyses reveal that the new scheme offers more effective security, better performance, and higher efficiency than Wu et al.'s scheme. We also provide a formal security proof of the protocol by using BAN authentication logic.

Keywords Wireless body area network (WBAN) · Authentication scheme · Security · Anonymity

Introduction

The aging problem worldwide, including our country, has been increasingly aggravated given the rapid economic development and constant progress in living standards and medical technologies. Statistics show that the average life expectancy for countries such as Japan, Switzerland, Singapore, and more than 20 other countries in 2015 is more than 80 years old [1]. A large number of elderly people impose a heavy burden on the family, society, and medical systems.

In 1996, Zimmerman [2] first proposed the concept of wireless body area network (WBAN), which has received a great deal of attention in academic and industrial fields. The relevant international standard for WBANs communication (i.e., IEEE 802.15.6) has been established along with four recommended security protocols [3]. However, these schemes still exhibit certain security flaws and are susceptible to network attacks [4, 5].

WBANs, as a notable application of the Internet of Things (IoT) technology, provide a simple and low-cost strategy for health monitoring and telemedicine of elderlies [6, 7].

As shown in Fig. 1, a typical medical WBAN application scenario is composed of a set of sensors implanted into or worn on the body to collect real-time patient health data, such as electrocardiography, electroencephalogram, electromyography, body temperature, heart rate, blood pressure, blood sugar and so on, and then send the collected biomedical data to remote telemedicine application providers. Doctors can monitor all indexes of patients, provide diagnosis, and offer curing guidance in real time through telemedicine

This article is part of the Topical Collection on *Systems-Level Quality Improvement*

✉ Dezhong Peng
pengdz@scu.edu.cn

Rui Chen
crs1934@hotmail.com

[1] College of Computer Science, Sichuan Normal University and College of Computer Science, Sichuan University, Chengdu, China

[2] College of Computer Science, Sichuan University, Chengdu, China

[3] Chengdu Ruibei Yingte Information Technology Limited Company, Chengdu, China

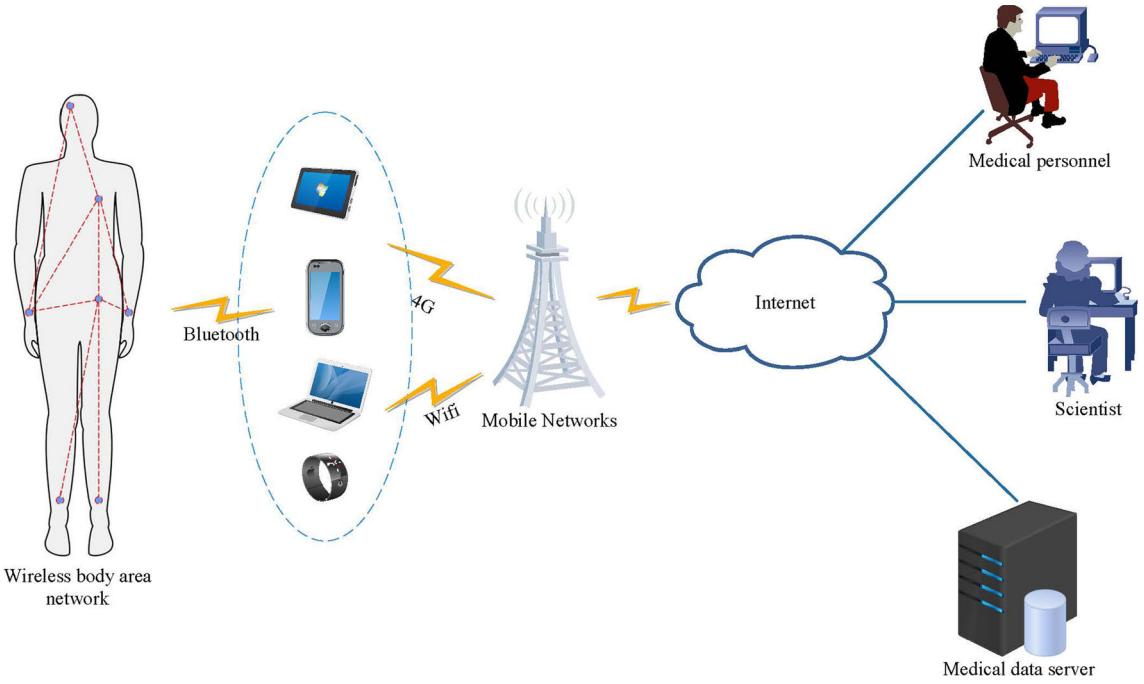

Fig. 1 A typical medical WBAN application scenario

systems. Owing to serious aging problems at present, the WBAN technology allows patients to be treated without leaving their homes and enables doctors to diagnose diseases and treat patients at medical institutions. Thus, WBAN has a significant application prospect and commercial value.

The completeness and accuracy of these data directly influence the medical behavior of doctors because the biological data collected by WBANs are used for remote clinical diagnosis. Moreover, the privacy of these data should be carefully protected [8]. Maliciously tampered health data may cause doctors to provide inaccurate assessments and diagnoses, which can lead to serious consequences. However, data transmission over the network is vulnerable to network attacks considering the openness of the network. Therefore, the primary goal of designing a secure mutual authentication protocol for WBANs is protecting user privacy while ensuring data accuracy, data integrity, and reliable connection.

Related works

Many authentication schemes for achieving this goal have been presented for WBANs in recent years. These schemes can achieve mutual authentication between the WBAN client (C) and the application provider (AP) and create shared session keys while realizing privacy protection and guarding the confidentiality and integrity of the data.

Jang et al. [9] summarized the security requirements of the WBAN, analyzed its security threats, and proposed a security framework for the WBAN. The schemes in [10, 11] are unsuitable for resource-limited sensor nodes because they are based on traditional public-key cryptosystems and require complex modular exponentiation between two communicating parties. Therefore, several schemes based on identity and elliptic curve cryptosystems (ECC) have been proposed [12–17]. These protocols do not require complex operations and user public-key certificate verification and management by not involving the public-key infrastructure and certificate authority, thereby simplifying the key management and computing costs.

However, these schemes are client-server mode authentication schemes (i.e., the network manager (NM) and AP are the same entity) and are susceptible to network attacks, thereby suggesting that these schemes are unsuitable for the application environment in WBANs.

Many certificateless authentication protocols have been proposed to enhance the communication security in WBANs [18–23]. In 2014, Liu et al. [18] presented two certificateless authentication schemes that use their own signature scheme for WBANs. He et al. [24] found that the schemes in [18] cannot prevent impersonation attacks and thus put forward a new authentication scheme for WBANs with provable security. Another scheme achieves user anonymity, and revocation was proposed in [19].

Zhao et al. [25] recently presented an ECC-based authentication protocol without pairing operations and

authentication tables for WBANs; however, the pseudo-identity of users in this scheme is a fixed value and cannot provide true user anonymity. Wang et al. [26] presented an improvement scheme that uses bilinear pairing and claimed that their scheme overcomes the limitations of the scheme in [25] and achieves user anonymity. However, an analysis revealed that Wang et al.'s scheme was also exposed to security flaws. The adversary can launch fraud attacks that impersonate legitimate C to communicate with APs, and a legal C can also impersonate another client to cheat the AP. The AP cannot identify and prevent the two types of attacks. Wu et al. [27] proposed a new efficient authentication scheme for WBANs to address these security drawbacks in [26]. Their scheme adopted one-side bilinear pairing operation, in which bilinear pairing operation was performed only on the AP side given the limited energy and computing power of the client. However, we find that Wu et al.'s scheme demonstrated numerous secure faults and that this scheme can neither prevent client impersonation attacks nor provide mutual authentication. The attackers could disguise themselves as a legitimate C to communicate with APs and illegally occupy network resources.

Contributions

The major contributions of this paper include: Firstly, through careful analysis, we indicate that Wu et al.'s scheme is still insecure against the impersonation attack. Secondly, we present an improved authentication scheme that uses asymmetric bilinear pairing to enhance the security of the original scheme, and proven its security with the BAN logic [29]. Finally, the result of comparison and analyses reveals that the new protocol can achieve many security features, such as user anonymity, privacy protection, mutual authentication, and session key establishment, while effectively withstanding various types of network attacks. Additionally, the proposed protocol inherits the one-side bilinear pairing operation of the original scheme, thereby reducing the computing costs of clients and making this scheme suitable for the application environment in WBANs.

Organization of this paper

The paper is structured as follows: The "Preliminaries" section introduces the study. The "Review of Wu et al.'s scheme" section discusses Wu et al.'s scheme and analyzes its security weakness. The "Proposed authentication scheme" section describes the presented authentication scheme for WBANs. The "Security analysis" section presents the analysis of the security of the new scheme. The "Performance analysis" section compares the performance of the proposed scheme with other recent works. The "Conclusion" Section draws several conclusions.

Preliminaries

Asymmetric bilinear pairings

Let G_1 and G_2 be two cyclic additive groups, while G_T is a cyclic multiplication group; their order is the same as the large prime q. Let $e : G_1 \times G_2 \rightarrow G_T$ be a pairing map. Thus, e is called a symmetric bilinear pairing (SBP) if $G_1 = G_2$ or asymmetric bilinear pairing (ABP) if $G_1 \neq G_2$. Obviously, SBP is a simplified form of ABP.

Most of the current authentication schemes generally apply the SBP method considering the simple implementation of this method. However, the SBP can only be obtained from Weil and Tate pairings on the supersingular elliptic curve. The maximum value of the safety factor k is only 6. The discrete logarithm problem under a certain attack (e.g., MOV attack [28]) can be transformed into a discrete logarithm problem over extended finite fields, thereby leading to a hidden security problem. Therefore, we constructed a new mutual authentication scheme for WBANs through ABP.

Related mathematical problems

Diffie-hellman (DH) problem Given $P \in G_1$ or G_2 and xP, compute for $x \in Z_q$.

Computational diffie-hellman (CDH) Problem For unknown $x, y \in Z_q$, $xyP \in G_1$ or G_2 should be computed given $P \in G_1$ or G_2 and xP, yP.

co-CDH problem For unknown $x, y \in Z_q$, $xyP_1 \in G_1$ should be computed given $P_1 \in G_1$ or G_2 and xP_1, yP_2.

Review of Wu et al.'s scheme

The following lists the notations used in this paper:

- q: a large prime order of groups;
- G_1, G_2: two cyclic additive group;
- G_T: a multiplicative group;
- P, P_1: a generator of G_1;
- P_2: a generator of G_2;
- e: a bilinear pairing map;
- h, h_1, h_2, h_3, h_4: one-way hash function;
- NM: the network manager;
- C: a WBAN client;

- AP: an application provider;
- $Enc_k(\cdot)/Dec_k(\cdot)$: a symmetric encryption/decryption algorithm with key k;

System initiation phase

In this process, the NM must complete a few steps to initiate the entire system:

1. NM first chooses a security parameter k. Let G_1 be a cyclic additive group generated by P, and G_T be a multiplicative group with the order q. Let $e : G_1 \times G_1 \rightarrow G_T$ be a bilinear pairing map. Computes $g = e(P, P)$. A randomly selected number $s_{NM} \in Z_q$, as the master key of NM, then NM calculates $Q_{NM} = s_{NM} \cdot P$ as its corresponding public key and then selects five security hash functions, $h : \{0,1\}^* \rightarrow Z_q, h_1 : \{0,1\}^* \times G_1 \times \{0,1\}^* \times V_C \rightarrow Z_q, h_2 : \{0,1\}^* \times G_1 \rightarrow Z_q, h_3 : \{0,1\}^* \rightarrow Z_q, h_4 : \{0,1\}^* \rightarrow Z_q$.
2. The NM publishes the tuple $\{k, q, P, G_1, G_T, e, g, h, h_1, h_2, h_3, h_4, Q_{NM}\}$ and keeps the s_{NM} undisclosed.

Registration phase

1. C transfers its identity ID_C to NM, then NM selects a random number $w_C \in Z_q$ and computes $W_C = w_C \cdot P, h_b = h_2(ID_C, W_C), \sigma_C = w_C + h_b \cdot s_{NM}$ after receiving the identity of C. Finally, the NM sends the private key (W_C, σ_C) to C through a secure transmission protocol.
2. AP transfers its identity ID_{AP} to NM, the NM generates a private key $s_{AP} = \frac{1}{s_{NM}+h(ID_{AP})} \cdot P$ for the AP after receiving ID_{AP}. Finally, the NM sends the private key s_{AP} to the AP through a secure transmission protocol.

Authentication phase

The C and AP should perform the following steps to achieve mutual authentication and generate a shared session key, as shown in Fig. 2:

(1) C randomly picks a number $r_C \in Z_q$ and a timestamp T_C, and computes $R_C = g^{rC}, K_C = r_C \cdot P, V_C = r_C \cdot (Q_{NM} + h(ID_{AP}) \cdot P), h_a = h_1(ID_C \parallel W_C \parallel R_C \parallel V_C), \sigma_C = r_C + \sigma_C \cdot h_a (\bmod q), Auth_C = Enc_{R_C}(ID_C \parallel T_C \parallel \sigma_C \parallel K_C \parallel W_C)$. Finally, C sends the message $M_1 = \{V_C, Auth_C, T_C\}$ to AP.

(2) AP first checks T_C upon receiving $\{V_C, Auth_C, T_C\}$ and terminates the session if it is invalid. Otherwise, AP computes $R_C^* = e(s_{AP}, V_C)$ and decrypts $Auth_C$ to obtain the $(ID_C, T_C, \sigma_C, K_C, W_C)$. Then AP computes $h_a^* = h_1(ID_C \parallel W_C \parallel R_C^* \parallel V_C), h_b = h_2(ID_C \parallel W_C)$ and verifies $\sigma_C \cdot P ? = K_C + h_a^* \cdot (W_C + Q_{NM} \cdot h_b)$. If the result is negative, then this message is dropped. Otherwise, AP selects a random number $r_{AP} \in Z_q$ and calculates $R_{AP} =$

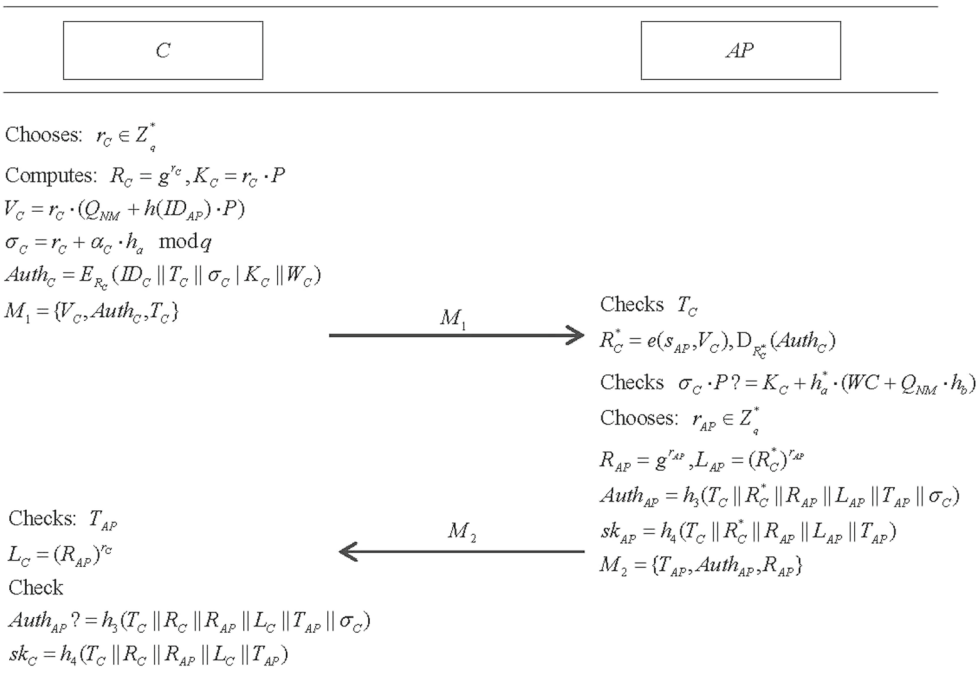

Fig. 2 The authentication phase of Wu et al.'s scheme

$g^{r_{AP}}, L_{AP} = (R_C^*)^{r_{AP}}, Auth_{AP} = h_3(T_C \parallel R_C^* \parallel R_{AP} \parallel L_{AP} \parallel T_{AP} \parallel \sigma_C)$, and the session key $sk_{AP} : sk_{AP} = h_4(T_C \parallel R_C^* \parallel R_{AP} \parallel L_{AP} \parallel T_{AP})$, where T_{AP} is the current timestamp. Finally, AP sends $M_2 = \{T_{AP}, Auth_{AP}, R_{AP}\}$ to the C as the response message.

(3) C first checks the T_{AP} upon receiving the reply message and terminates the session if it is not valid. Then C computes $L_C = (R_{AP})^{r_C}$ and checks whether $Auth_{AP}$ is equal to $h_3(T_C \parallel R_C \parallel R_{AP} \parallel L_C \parallel T_{AP} \parallel \sigma_C)$. If the result is equal, then C computes the shared session key $sk_C = h_4(T_C \parallel R_C \parallel R_{AP} \parallel L_C \parallel T_{AP})$.

Security weakness of Wu et al.'s scheme

Wu et al. [27] stated that their scheme can satisfy many security requirements. However, we reveal that their scheme is unsafe and suffers from impersonation attacks. An adversary could easily impersonate the identity of legal clients to deceive AP by performing the following steps:

(1) Suppose A is an attacker, he/she randomly selects an identity ID_A, a timestamp T_A, and three random numbers $r_A, x_A, w_A \in Z_q$. Then, A performs the following calculation:

$$\begin{aligned} R_A &= g^{r_A}, X_A = x_A \cdot P, W_A = w_A \cdot P \\ V_A &= r_A(Q_{NM} + h(ID_{AP}) \cdot P) \\ h_a &= h_1(ID_A \parallel W_A \parallel R_A \parallel V_A) \\ h_b &= h_2(ID_A \parallel W_A) \\ \sigma_A &= x_A K_A = X_A - h_A(W_A + Q_{NM} \cdot h_b) \\ Auth_A &= Enc_{R_A}(ID_A \parallel T_A \parallel \sigma_A \parallel K_A \parallel W_A) \end{aligned}$$

(2) A sends $M_1 = \{V_A, Auth_A, T_A\}$ to AP.

(3) AP first checks the validation of T_A after receiving M_1 and computes

$$\begin{aligned} R_A^* &= e(s_{AP}, V_A) \\ &= e\left(\frac{1}{s_{NM}+h(ID_{AP})} \cdot P, r_A \cdot (Q_{NM}+h(ID_{AP}) \cdot P)\right) \\ &= e\left(\frac{1}{s_{NM}+h(ID_{AP})} \cdot P, r_A \cdot (s_{NM}+h(ID_{AP})) \cdot P\right) \\ &= e(P, P)^{\frac{1}{s_{NM}+h(ID_{AP})} \cdot r_A \cdot (s_{NM}+h(ID_{AP}))} \\ &= e(P, P)^{r_A} \\ &= g^{r_A} = R_A \end{aligned}$$

Then, AP obtains $\{ID_A, T_A, \sigma_A, K_A, W_A\}$ by encrypting $Auth_A$ and computes $h_b = h_2(ID_A \parallel W_A)$. Next, AP computes $\sigma_A \cdot P$ and checks whether it is equal to $K_A + h_A^*(W_A + Q_{NM} \cdot h_b)$. If not, then AP rejects the message.

Note that the message σ_A can pass the verification of AP because

$$\begin{aligned} \sigma_A \cdot P &= x_A \cdot P = X_A \\ & K_A + h_A^*(W_A + Q_{NM} \cdot h_b) = X_A - h_A(W_A + Q_{NM} \cdot h_b) \\ & + h_A^*(W_A + Q_{NM} \cdot h_b) = X_A \end{aligned}$$

Thus, we can obtain $\sigma_A \cdot P = K_A + h_A^*(W_A + Q_{NM} \cdot h_b)$

Finally, the message $M_1 = \{V_A, Auth_A, T_A\}$ can successfully pass the verification. The AP believes that adversary A is a legal C. Therefore, Wu et al.'s scheme cannot provide mutual authentication and resistance to impersonation attacks.

Proposed authentication scheme

From the above analysis, it is shown that the scheme of Wu et al. cannot resist client impersonation attacks and achieve mutual authentication. In order to resolve this problem and provide a better solution, in this section we propose an improved authentication scheme based on Wu et al.'s scheme, which inherits and develops the merits of the original scheme such as symmetric encryption and one-side bilinear pairing operation.

Furthermore we also introduce ABP which can provide more secure authentication than SBP, this makes the new scheme more secure than related works.

System initiation phase

The system initiation phase has the following steps:

1. NM first selects a security parameter k. Let G_1 and G_2 be a cyclic additive group, and their generators are P_1 and P_2, respectively. Let G_T be a multiplicative group. G_1, G_2, and G_T have the same large prime order q. Let $e : G_1 \times G_2 \rightarrow G_T$ be a bilinear pairing map that computes $g = e(P_1, P_2)$. A randomly selected number $s_{NM} \in Z_q$ as the master key of NM, then NM calculates $PK_1 = s_{NM} \cdot P_1, PK_2 = s_{NM} \cdot P_2$ as its corresponding public key and selects the following hash functions: $h : \{0,1\}^* \rightarrow Z_q, h_1 : \{0,1\}^* \times G_1 \rightarrow Z_q$, $h_2 : \{0,1\}^* \times \{0,1\}^* \times G_1 \times G_T \times G_1 \times G_2 \rightarrow Z_q$, $h_3 : \{0,1\}^* \times \{0,1\}^* \times G_1 \times G_1 \times G_T \rightarrow \{0,1\}^*$, $h_4 : G_1 \times G_1 \times G_T \times \{0,1\}^* \rightarrow \{0,1\}^*$.
2. The NM publishes the tuple $\{k, q, P_1, P_2, G_1, G_2, G_T, e, g, h, h_1, h_2, h_3, h_4, PK_1, PK_2\}$ and keeps the s_{NM} undisclosed.

Registration phase

1. C transfers its identity ID_C to NM, then NM picks a random number $w_C \in Z_q$ and computes $W_C = w_C \cdot P_1, h_C = h_1(ID_C \parallel W_C), s_C = w_C + s_{NM} \cdot h_C$ as the private key of C. Finally, the NM securely sends (W_C, s_C) to C.
2. AP transfers its identity ID_{AP} to NM, the NM generates $s_{AP} = \frac{1}{s_{NM} h(ID_{AP})} \cdot P_1$ as the private key of AP. Finally, the NM securely sends s_{AP} to the AP.

Authentication phase

An authentication phase is performed when C aims to link the AP and negotiate a session key. The authentication process is depicted in Fig. 3. The detailed steps are listed below:

(1) C selects a random number $r_C \in Z_q$, obtains the current timestamp T_C, and then computes $R_C = g^{r_C}, K_C = r_C \cdot P_1, V_C = r_C \cdot h(ID_{AP}) \cdot PK_2, Q_C = h_2(ID_C \parallel T_C \parallel W_C \parallel R_C \parallel K_C \parallel V_C), \sigma_C = r_C + s_C \cdot Q_C (\bmod q), Auth_C = Enc_{R_C}(ID_C \parallel T_C \parallel \sigma_C \parallel W_C \parallel K_C)$. Finally, C sends $M_1 = \{V_C, Auth_C, T_C\}$ to the AP.

(2) AP first checks T_C upon receiving $M_1 = \{V_C, Auth_C, T_C\}$ and discards the message if it is invalid. Otherwise, AP calculates $R_C^* = e(s_{AP}, V_C)$ and decrypts $Auth_C : Dec_{R_C^*}(Auth_C) = \{ID_C, T_C, \sigma_C, W_C, K_C\}$. The AP computes $Q_C^* = h_2(ID_C \parallel T_C \parallel W_C \parallel R_C^* \parallel K_C \parallel V_C)$ and the public key of C: $PK_C = W_C + PK_1 \cdot h_1(ID_C \parallel W_C)$. Then, the AP verifies $\sigma_C \cdot P_1 ? = K_C + PK_C \cdot Q_C^*$. If the result is negative, then this message is dropped. Otherwise, the AP selects a random number $r_{AP} \in Z_q$ and then calculates $R_{AP} = r_{AP} \cdot P_1, L_{AP} = r_{AP} \cdot K_C$ and the session key $sk_{AP} : sk_{AP} = h_3(ID_C \parallel ID_{AP} \parallel L_{AP} \parallel R_{AP} \parallel R_C^*)$. Finally, the AP computes $Auth_{AP} = h_4(L_{AP} \parallel R_{AP} \parallel R_C^* \parallel sk_{AP})$ and sends $M_2 = \{R_{AP}, Auth_{AP}\}$ to the C as the response message.

(3) The C computes $L_{AP}^* = r_C \cdot R_{AP}$ and the shared session key $sk_C = h_3(ID_C \parallel ID_{AP} \parallel L_{AP}^* \parallel R_{AP} \parallel R_C)$ upon receiving the reply message. Then, C checks if the equation $Auth_{AP} ? = h_4(L_{AP}^* \parallel R_{AP} \parallel R_C \parallel sk_C)$ holds. If they are equal, then the C and AP complete the mutual authentication, and a secure communication channel is established using $sk_{AP} = sk_C = h_3(ID_C \parallel ID_{AP} \parallel L_{AP} \parallel R_{AP} \parallel R_C)$.

Security analysis

We first give the security analysis of the improvement scheme by using BAN logic [29]. Then, we demonstrate that the new scheme can achieve higher security features than those in previous works.

Authentication proof using BAN logic

Some notations are listed below:

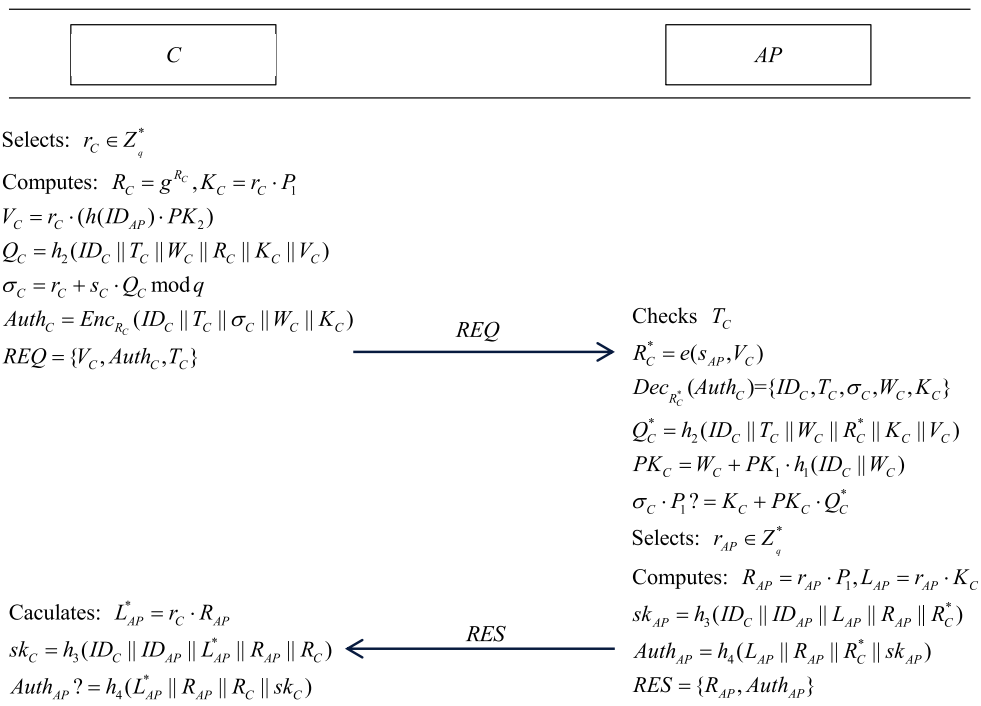

Fig. 3 The authentication phase of our scheme

P, Q: two principals;
X, Y: two statements;
$P|\equiv X$: P believes X;
$\#(X)$: X is fresh;
$P \Rightarrow Q$: P has jurisdiction over X;
$P \lhd Q$: P says X;
$P|\sim Q$: P once said X;
(X, Y): X or Y is one part of (X, Y);
$(X)_K$: X is hash with the key K;
$\{X\}_K$: X is cipher with the key K;
$\langle X\rangle_Y$: X with the secret K;
$P \overset{K}{\longleftrightarrow} Q$: P and Q use the shared key K to communication;
$P \overset{K}{\rightleftharpoons} Q$: K is the shared secret between P and Q;

The implantation of BAN logic typically requires four steps as follows: idealizing the proposed scheme; formulating assumptions, setting goals; and analyzing the protocol.

(1) The idealized forms of the transmitted messages are as follows:

$M_1: \quad C \rightarrow AP : \{ID_C, T_C, K_C, \sigma_C, W_C\}_K$ where $K = R_C = R_C^* = e(P_1, P_2)^{r_C}$

$M_2: \quad AP \rightarrow C : \{ID_C, ID_{AP}, R_{AP}, C \overset{sk}{\longleftrightarrow} AP\}_K$

(2) Several assumptions are listed as follows to analyze the proposed protocol:

$A_1: \quad C \mid\equiv \#(r_{AP})$
$A_2: \quad AP \mid\equiv \#(T_C)$
$A_3: \quad C \mid\equiv C \overset{K}{\longleftrightarrow} AP$
$A_4: \quad AP \mid\equiv C \overset{K}{\longleftrightarrow} AP$
$A_5: \quad C \mid\equiv AP \Rightarrow C \overset{K}{\longleftrightarrow} AP$
$A_6: \quad AP \mid\equiv C \Rightarrow C \overset{K}{\longleftrightarrow} AP$
$A_7: \quad AP \mid\equiv C \Rightarrow C \overset{ID_C}{\longleftrightarrow} AP$

(3) According to the analytic procedures of BAN logic, the verification goals of the proposed protocol are listed below:

$G_1: \quad C \mid\equiv C \overset{sk}{\longleftrightarrow} AP$
$G_2: \quad C \mid\equiv AP \mid\equiv C \overset{sk}{\longleftrightarrow} AP$
$G_3: \quad AP \mid\equiv C \overset{sk}{\longleftrightarrow} AP$
$G_4: \quad AP \mid\equiv C \mid\equiv C \overset{sk}{\longleftrightarrow} AP$

(4) We analyze the idealized form of the new protocol based on the above assumptions and the rules of BAN logic as follows:

From M_1, we have

$S_1 : AP \lhd \{ID_C, T_C, \sigma_C, W_C, K_C\}_K$

From S_1 and A_4 and the message-meaning rule, we obtain:

$S_2 : AP|\equiv C|\sim \{ID_C, T_C, \sigma_C, W_C, K_C\}$

From S_2 and A_2 and the freshness conjuncatenation rule, we obtain:

$S_3 : AP|\equiv C|\equiv \{ID_C, T_C, \sigma_C, W_C, K_C\}$

From S_3, we have

$S_4 : AP|\equiv C|\equiv \{ID_C, K_C\}$

From S_4 and the message-meaning rule, we obtain:

$S_5 : AP|\equiv C|\equiv \{ID_C\}$

$S_6 : AP|\equiv C|\equiv \{K_C\}$

From $L_{AP} = r_{AP} \cdot K_C$ and $sk = h_3(ID_C \parallel ID_{AP} \parallel L_{AP} \parallel R_{AP} \parallel R_C^*)$, we obtain:

$S_7 : AP \mid\equiv C \mid\equiv C \overset{sk}{\longleftrightarrow} AP \ (G_4)$

From S_7 and A_6 and the jurisdiction rule, we obtain:

$S_8 : AP \mid\equiv C \overset{sk}{\longleftrightarrow} AP \ (G_3)$

From M_2, we obtain:

$S_9 : C \lhd \{ID_C, ID_{AP}, R_{AP}, C \overset{sk}{\longleftrightarrow} AP\}_K$

From S_9 and A_3 and the message-meaning rule, we obtain:

$S_{10} : C|\equiv AP|\sim \{ID_C, ID_{AP}, R_{AP}, C \overset{sk}{\longleftrightarrow} AP\}$

From S_{10}, A_1, $R_{AP} = r_{AP} \cdot P_1$, and the freshness conjuncatenation rule , we obtain:

$S_{11} : C|\equiv AP|\equiv \{ID_C, ID_{AP}, R_{AP}, C \overset{sk}{\longleftrightarrow} AP\}$

From S_{11}, we obtain:

$S_{12} : C|\equiv AP|\equiv C \overset{sk}{\longleftrightarrow} AP \ (G_2)$

From S_{12}, A_5 and the jurisdiction rule, we obtain:

$S_{13} : C|\equiv C \overset{sk}{\longleftrightarrow} AP \ (G_1)$

Security features analysis

Mutual authentication and key agreement

In the proposed protocol, C and AP can authenticate each other given the DL and CDH problems and the equation:

$$\begin{aligned} R_C^* &= e(s_{AP}, V_C) \\ &= e(\frac{1}{s_{NM} h(ID_{AP})} \cdot P_1, r_C \cdot (h(ID_{AP}) \cdot PK_2)) \\ &= e\left(\frac{1}{s_{NM} h(ID_{AP})} \cdot P_1, r_C \cdot (h(ID_{AP}) \cdot s_{NM} \cdot P_2)\right) \\ &= e(P_1, P_2)^{\frac{1}{s_{NM} h(ID_{AP})} \cdot r_C \cdot h(ID_{AP}) s_{NM}} \\ &= e(P_1, P_2)^{r_C} \\ &= g^{r_C} = R_C \end{aligned}$$

and

$$\begin{aligned} L^*_{AP} &= r_C \cdot R_{AP} \\ &= r_C r_{AP} \cdot P_1 \\ &= r_{AP} \cdot K_C = L_{AP} \end{aligned}$$

According to the two equations, C and AP can compute the same session key as follows:

$$\begin{aligned} sk_{AP} &= h_3(ID_C \| ID_{AP} \| L_{AP} \| R^*_C) \\ &= h_3(ID_C \| ID_{AP} \| L^*_{AP} \| R_C) \\ &= sk_C \end{aligned}$$

According to the DL and CDH problems, only the legitimate C and AP can generate the correct message $REQ = \{V_C, Auth_C, T_C\}$ and $RES = \{R_{AP}, Auth_{AP}\}$ and compute the same session key.

Thus, the new protocol can achieve mutual authentication and key establishment between C and AP.

User anonymity and untraceability

The identity of C is contained in $s_C = w_C + s_{NM} \cdot h_1(ID_C \| W_C)$ and the ciphertext $Auth_C = Enc_{R_C}(ID_C \| T_C \| \sigma_C \| W_C \| K_C)$. The ID_C cannot be extracted from the hash value $h_1(ID_C||W_C)$. Moreover, the adversary cannot decrypt $Auth_C$ to obtain ID_C without R_C, which can be computed only by $R_C = g^{r_C}$ or $R^*_C = e(s_{AP}, V_C)$. The adversary cannot obtain r_C and s_{AP} because r_C is a random value and s_{AP} is the secret key of the AP, and then generates R_C or R^*_C. In the proposed protocol, every new login request message of the C includes a new random number $r_C \in Z_q$, and every reply message of the AP includes new random number $r_{AP} \in Z_q$. Owing to the random number r_C and r_{AP}, the communication messages $REQ = \{V_C, Auth_C, T_C\}$ and $RES = \{R_{AP}, Auth_{AP}\}$ are different every time and unlinkable. The adversary cannot find the link among messages and links it to C or traces the moving history and path.

Therefore, the proposed protocol supports user anonymity and untraceability.

Perfect forward secrecy

The temporary parameters (i.e., r_C and r_{AP}) in our protocol are selected randomly by the C and AP, respectively. The adversary can generate $e(s_{AP}, V_C) = g^{r_C}$ and obtain $R_{AP} = r_{AP} \cdot P_1$, even though the secret key of C or AP is compromised by the adversary. However, he/she cannot obtain r_C and r_{AP} and thus computes $L_{AP} = r_{AP} \cdot K_C$ through g^{r_C}, $r_{AP} \cdot P_1$ or $r_{AP} \cdot K_C$, which is a CDH problem. Moreover, the session key between C and AP will not be leaked, even if the secret keys of the NM are compromised, because the session key contains a random number.

Therefore, our improvement protocol provides perfect forward secrecy.

Resist known attacks

The proposed scheme can provide good security and resist various known attacks:

1. Resist replay attack:
   The AP can quickly detect the replay attack by checking T_C because the login request message $REQ = \{V_C, Auth_C, T_C\}$ contains the timestamp T_C. The tampering of T_C also cannot pass the verification because $Auth_C$ contains T_C. The reply message contains the random data R_C and R_{AP}. Thus, C can easily find replay attacks by checking these data.
2. Resist message tamper attack:
   The login request message includes the signature $\sigma_C = r_C + s_C \cdot Q_C$ where $Q_C = h_2(ID_C \| T_C \| W_C \| R_C \| K_C \| V_C)$. If the adversary tampers the login message, then the AP can easily detect the tamper attack by verifying σ_C. Moreover, the C can find the tamper attack by $Auth_{AP}? = h_4(L^*_{AP} \| R_{AP} \| R_C \| sk_C)$ if the adversary tampers the reply message because only a legal AP can obtain $\{R_C, K_C\}$ and generate the correct L_{AP}.
3. Resist impersonation attacks
   C-impersonation attacks: Suppose the adversary impersonates C and randomly selects an identity ID_A and timestamp T_A, the login request message $REQ = \{V_A, Auth_A, T_A\}$ is generated. Finally, A sends REQ to AP. The AP first computes $R^*_A = e(s_{AP}, V_A) = g^{r_A} = R_A$ upon receiving the message and then decrypts $Auth_A : Dec_{R_A}(Auth_A) = \{ID_A, T_A, \sigma_A, W_A, K_A\}$. Then, the AP computes $Q^*_C = h_2(ID_A \| T_A \| W_A \| R^*_A \| K_A \| V_A)$, $PK_A = W_A + PK_1 \cdot h_1(ID_A \| W_A)$ and verifies $\sigma_A \cdot P_1? = K_A + PK_A \cdot Q^*_C$. The adversary cannot generate a legal σ_A given the lack of a legal secret key. The modification of K_A will result in the change of Q^*_C and lead to $Q^*_C \neq Q_C$. Thus, AP can find this attack by verifying $\sigma_A \cdot P_1? = K_A + PK_A \cdot Q^*_C$.

AP-impersonation attacks: Suppose an adversary A impersonates AP, A can generate R_{AP} but cannot compute legal $Auth_{AP} = h_4(L_{AP} \| R_{AP} \| R^*_C \| sk_{AP})$. A cannot directly compute the legal R_C and further obtain

Table 1 Running time of related operations (MS)

	T_{BP}	T_{SM}	T_{ME}
AP	20.04	6.38	13.21
C	96.35	30.67	63.51

Table 2 Comparisons of computation cost (MS)

	C	AP	Total time
Wang et al.'s scheme [26]	$3T_{SM} + T_{BP} = 188.36$	$2T_{SM} + T_{BP} = 32.8$	221.16
Wu et al.'s scheme [27]	$3T_{SM} + 2T_{ME} = 219.03$	$3T_{SM} + 2T_{ME} + T_{BP} = 65.8$	284.83
Our scheme	$3T_{SM} + T_{ME} = 155.52$	$5T_{SM} + T_{BP} = 51.94$	207.46

$\{ID_C, T_C, \sigma_C, W_C, K_C\}$, even if A intercepts the login request message $REQ = \{V_C, Auth_C, T_C\}$ of C. Finally, A cannot compute legal K_C, L_{AP}, sk_{AP} and $Auth_{AP}$. C can detect this type of attack by verifying $Auth_{AP}? = h_4(L^*_{AP} \| R_{AP} \| R_C \| sk_C)$.

Performance analysis

We briefly compare the performance of the proposed protocol with the scheme of Wang et al. [26] and Wu et al. [27] in terms of computation and communication costs.

Computation cost

Several of the following symbols are defined to illustrate the performance comparisons:

- T_{ME}: Time cost for a modulus exponentiation
- T_{BP}: Time cost for a bilinear pairing operation
- T_{SM}: Time cost for scalar multiplication based on pairing

Table 1 summarizes the execution time of the bilinear pairing based on the experimental data in [18]. Several operations, such as point addition and one-way hash, were omitted because of the minimal time cost. Table 2 gives the comparisons result of performance between the new protocol and two other relevant protocols. In this table, the total computation cost of the proposed protocol is 207.46 ms, which is slightly less than that of the schemes of Wang et al. and Wu et al.. In comparison with the schemes proposed by Wang et al. and Wu et al., the total execution time of C and AP in our protocol was decreased by 6.2% and 27.2%, correspondingly.

Communication cost

In the simulation, we assumed that the size of p is 64 bytes, and the element in G_1 and G_2 is 128 bytes, and the size of q was 20 bytes. We suppose that the length of the output of all hash functions and identities is 20 bytes, and the length of the timestamp is 4 bytes. The exchanged messages of the two communicating parties in our proposed scheme were $M_1 = \{V_C, Auth_C, T_C\}$ and $M_2 = \{R_{AP}, Auth_{AP}\}$, where $Auth_C = Enc_{K_C}(ID_C \| T_C \| \sigma_C \| W_C \| K_C)$ and $Auth_{AP} = h_4(L_{AP} \| R_{AP} \| R^*_C \| sk_{AP})$. Thus, the total size was 856 bytes. We also computed the communication cost of the scheme of Wang et al. and Wu et al. at 828 and 976 bytes, respectively.

These data indicated that the communication cost is higher in the new scheme than in Wang et al.'s scheme but lower than that of Wu et al.'s scheme.

Conclusion

The aggravating problems caused by the elderly population have become an important topic worldwide. Telemedicine systems based on WBANs are an effective means of solving this problem. In this paper, we first review the recent studies on WBANs and analyze an anonymous authentication scheme of Wu et al. We demonstrate that their scheme is unsafe and suffers from impersonation attacks. An adversary can access the network service by cheating AP through a randomly selected identity. We then put forward an improvement authentication protocol for WBANs based on ABP. The correlation analysis indicate that our protocol can provide a reliable security and withstand various network threats. The proposed scheme exhibit superior performance over previous protocols, thereby suggesting that the proposed scheme is feasible for WBAN environments with limited power and resources.

Acknowledgements This work was supported in part by the National Natural Science Foundation of China under grants U1435213 and 61172180, and Chengdu International Cooperation Project under grants 2016-GH02-00048-HZ and 2015-GH02-00041- HZ, and General Project of Education Department in Sichan under grants 18ZB0485.

Funding information This study was funded by National Natural Science Foundation of China (grant number U1435213 and 61172180), and Chengdu International Cooperation Project (grant number 2016-GH02-00048-HZ and 2015-GH02-00041-HZ), and General Project of Education Department in Sichuan (grant number 18ZB0485).

Compliance with ethical standards

Conflict of interests Author Dezhong Peng has received research grants from National Natural Science Foundation of China and Chengdu International Cooperation Project. Author Rui Chen has received research grants from General Project of Education Department in Sichuan. Author Dezhong Peng declares that he has no conflict of interest. Author Rui Chen declares that he has no conflict of interest.

Ethical approval This article does not contain any studies with human participants performed by any of the authors.

References

1. WHO, Life expectancy increased by 5 years since 2000, but health inequalities persist. *Saudi Med. J.* 37(6):717–717, 2016.
2. Zimmerman, T. G., Personal area networks: near-field intrabody communication. *IBM Syst. J.* 35(3/4):609–617, 1996.
3. Ieee standard for local and metropolitan area networks - part 15.6: Wireless body area networks in IEEE Std, 2012.
4. Toorani, M., On vulnerabilities of the security association in the ieee 802.15.6 standard. In: *International conference on financial cryptography and data security*, pp. 245–260, 2015.
5. Toorani, M., Security analysis of the ieee 802.15.6 standard. *Int. J. Commun. Syst.* 29(17):2471–2489, 2016.
6. Monton, E., Hernandez, J. F., Blasco, J. M., and Hervé, T., Body area network for wireless patient monitoring. *IET Commun.* 2(2):215–222, 2008.
7. Seyedi, M., Kibret, B., Lai, D. T., and Faulkner, M., A survey on intrabody communications for body area network applications. *IEEE Trans. Biomed. Eng.* 60(8):2067–79, 2013.
8. He, D., Zeadally, S., and Wu, L., Certificateless public auditing scheme for cloud-assisted wireless body area networks. *IEEE Syst. J.* PP(99):1–10, 2015.
9. Jang, C. S., Lee, D. G., and Han, J. W., A proposal of security framework for wireless body area network. In: *International conference on security technology*, pp. 202–205, 2008.
10. Rivest, R. L., Shamir, A., and Adleman, L., A method for obtaining digital signatures and public-key cryptosystems. *Communications of the Acm* 21(2):120–126, 1978.
11. Elgamal, T., A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* 31(4):469–472, 1984.
12. He, D., and Zeadally, S., Authentication protocol for ambient assisted living system. *IEEE Commun. Mag.* 35(1):71–77, 2015.
13. He, D., Kumar, N., Chen, J., Lee, C. C., Chilamkurti, N., and Yeo, S. S., Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. *Multimed. Syst.* 21(1):49–60, 2015.
14. He, D., Kumar, N., and Chilamkurti, N., A secure temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. *Int. Symposium Wireless Pervasive Comput.* 321(1):263–277, 2015.
15. He, D., and Wang, D., Robust biometrics-based authentication scheme for multiserver environment. *IEEE Syst. J.* 9(3):816–823, 2015.
16. Huang, X., Xiang, Y., Bertino, E., Zhou, J., and Xu, L., Robust multi-factor authentication for fragile communications. *IEEE Trans. Dependable Secure Comput.* 11(6):568–581, 2014.
17. Drira, W., Renault, E., and Zeghlache, D., A hybrid authentication and key establishment scheme for wban. In: *IEEE international conference on trust, security and privacy in computing and communications*, pp. 78–83, 2012.
18. Liu, J., Zhang, Z., Chen, X., and Kwak, K. S., Certificateless remote anonymous authentication schemes for wirelessbody area networks. *IEEE Trans. Parallel Distrib. Syst.* 25(2):3332–342, 2014.
19. Xiong, H., and Qin, Z., Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. *IEEE Trans. Inf. Forensics Secur.* 10(7):1442–1455, 2015.
20. Al-Riyami, S. S., and Paterson, K. G., Certificateless public key cryptography. In: *International conference on the theory and application of cryptology and information security*, pp. 452–473, 2003.
21. Xiong, H., Cost-effective scalable and anonymous certificateless remote authentication protocol. *IEEE Trans. Inf. Forensics Secur.* 9(12):2327–2339, 2014.
22. Zhang, L., Liu, J., and Sun, R., An efficient and lightweight certificateless authentication protocol for wireless body area networks. In: *International conference on intelligent networking and collaborative systems*, pp. 637–639, 2013.
23. Kang, B., Wang, J., and Shao, D., Certificateless public auditing with privacy preserving for cloud-assisted wireless body area networks, Mobile Information Systems 2017(2017-7-6), 2017.
24. He, D., Zeadally, S., Kumar, N., and Lee, J. H., Anonymous authentication for wireless body area networks with provable security. *IEEE Syst. J.* PP(99):1–12, 2016.
25. Zhao, Z., An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. *J. Med. Syst.* 38(2):1–7, 2014.
26. Wang, C., and Zhang, Y., New authentication scheme for wireless body area networks using the bilinear pairing. *J. Med. Syst.* 39(11):1–8, 2015.
27. Wu, L., Zhang, Y., Li, L., and Shen, J., Efficient and anonymous authentication scheme for wireless body area networks. *J. Med. Syst.* 40(6):1–12, 2016.
28. Menezes, A. J., Okamoto, T., and Vanstone, S. A., Reducing elliptic curve logarithms to logarithms in a finite field. In: *ACM symposium on theory of computing*, pp. 80–89, 1991.
29. Burrows, M., Abadi, M., and Needham, R., A logic of authentication. *ACM Sigops Operating Systems Review* 8(1):18–36, 1990.