Journal of Information Hiding and Privacy Protection
DOI:10.32604/jihpp.2020.09901
Article

Tech Science Press

Design of a Mutual Authentication and Key Agreement Protocol for WBANs

Xiangwei Meng, Jianbo Xu[*], Xiaohe Wu and Zhechong Wang

School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, 411105, China
[*]Corresponding Author: Jianbo Xu. Email: jbxu@hnust.edu.cn

Received: 25 July 2020; Accepted: 21 August 2020

Abstract: Please WBANs are a sensor network for detection and collection of sensitive data to the human body, which is lightweight and mobile. WBANs transmit sensitive and significant messages through the public channel, which makes it easy for an attacker to eavesdrop and modify the messages, thus posing a severe threat to the security of the messages. Therefore, it is essential to put in place authentication and key agreement between different communication nodes in WBANs. In this paper, a lightweight and secure authenticated key agreement protocol in wireless body area networks is designed. It is capable to reduce the cost of sensor node computation while ensuring security. Besides, an informal security analysis is conducted to discuss the security of the protocol against well-known attacks. Finally, the energy consumption of the protocol is evaluated, and the results show that the sensor nodes only need low storage cost, computational cost and communication cost.

Keywords: WBANs; lightweight; mutual authentication; key agreement

1 Introduction

In recent years, with the rapid development of microelectronics technology and network technology, new technologies represented by the Internet of Things have emerged [1–3]. The Internet of Things is an application network that combines information sensing devices with the Internet and has a wide range of applications, for example, intelligent transport, smart home, healthcare and so on. Wireless Body Area Networks (WBANs) is the specific application of the Internet of Things in respect of healthcare services [4–5]. WBANs consists of multiple sensor devices that are implanted in or worn on the body. Each sensor device is used to collect physiological data of the patient, and the collected data is then transmitted to the medical service provider through a public channel. The medical service provider processes the collected data according to the needs of the user [6]. WBANs are capable of monitoring the biological functions of patients in full time domain without restricting the free movement of patients, such as blood pressure, heart rate, blood sugar and so on. It can reduce the cost of medical monitoring while facilitating the medical treatment received by patients, which is conducive to reducing the medical burden placed on society. The message transmitted in WBANs contains significant and sensitive physiological data of patients. How to realize the secure transmission of physiological data on patients in public channel is an urgent problem to be resolved [7]. Due to volume constraint, sensor devices are incapable of performing complex calculations. Besides, their storage space is limited. Therefore, the security mechanism of WBANs is required to ensure information security and lightweight at the same time [8].

1.1 Related Work

In 2014, Liu et al. [9] proposed two WBAN certificate less remote anonymous authentication schemes. However, Zhao [10] indicated that the scheme [9] came up with could not protect against theft-launched certification attack and then proposed an enhanced solution. In the same year, Xiong et al. [11] discovered that Liu's scheme certificate management was lacking in efficiency, scalability and forward secrecy. Therefore, they proposed a scalable anonymous certificate less remote authentication protocol for WBANs, which not only improved security performance, but also reduced the workload of communication and computation.

In 2017, Li et al. [12] proposed a centralized two-hop lightweight anonymous mutual authentication and key agreement scheme in WBANs, which allows the connection of sensor nodes to the patient's body for authentication by the local server. The session key is established in a way that is anonymous and unlinkable. Nevertheless, the protocol shows flaws in respect of anonymity and unlinkability.

In 2018, Ostad-Sharif et al. [13] found out that the scheme proposed by Li et al. [12] is incapable of withstanding the key replicating attack. Ostad-Sharif et al. [13] put forward a new scheme to compensate for the key replication attack vulnerability in the sensor node with as few as four hash functions. However, this solution remains incapable of defending against sensor node capture attack.

2 System Model

2.1 Network Model

The network model of WBANs is illustrated in Fig. 1, which contains a two-layer network. The first layer network is the Intra-BAN purposed to collect and forward the physiological data collected from the patient, and is comprised of a multitude of sensor nodes and intermediate nodes. The sensor node performs an information-aware function that is responsible for the collection of physiological data from the patient. However, the constraint of energy consumption makes it unlikely to establish communication with the hub node straightaway. Besides, there is only the intermediate node that is responsible for data forwarding. The intermediate node has a superior communication capability to the sensor node. In the network, it is only responsible for forwarding data between the sensor node and the hub node, for which it does not get involved in the encryption of the forwarded data. The second layer network is an Inter-BAN responsible for receiving data sent by the first layer network, as well as storing and applying the received data. The hub node is a server node in the network, as well as a node connecting the WBANs and the Beyond-BAN. That is to say, it is responsible for collecting data from Intra-BAN and transmitting data to Beyond-BAN's medical service provider. The hub node has the most robust capability with regard to computation, storage capacity and communication [14].

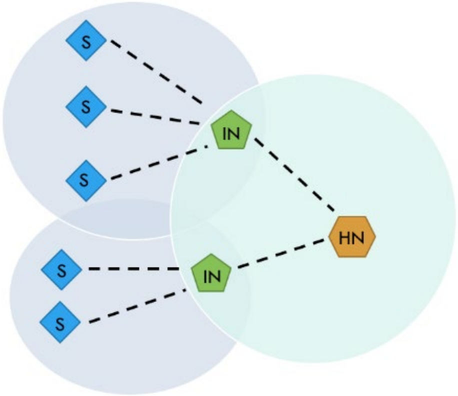


Figure 1: Network model of WBANs

2.2 Adversary Model

Applying the well-known Dolev-Yao threat model [15], the attacker is able to eavesdrop, intercept, and revise all message transmitted through a public channel. The attacker can capture any sensor node and steal all the information stored in the memory of that node. The sensor node registration information in the hub node memory is incapable to be acquired by the attacker. System administrators are fully trustworthy.

3 The Proposed Protocol

The proposed protocol is divided into three phases: Initialization phase, registration phase and authentication phase. The initialization phase and the registration phase are executed by the *SA*. The notations used in the protocol are shown in Tab. 1.

Table 1: Notations used in this protocol

Notation	Description
SA	System administrator
S	Sensor node
IN	Intermediate node
HN	Hub node
ID_S	Secret biometric identity of *S*
TID_S	Temporary identity of *S*
ID_{IN}	Permanent identity of *IN*
K_{HN}	Master secret key of *HN*
K_S	Session key
H_1, H_2	Authentication parameters
a	Temporary secret parameter picked by *SN*
A_S, B_S	Temporary secret parameters
T_1, T_2	Timestamps
$\oplus$	Bitwise XOR operation
h (.)	One-way hash function

3.1 Initialization Phase

Step A1: Picks a *HN*'s master secret key K_{HN}.

Step A2: Stores the K_{HN} into the *HN*'s memory.

3.2 Registration Phase

Step B1: Acquires the patient's secret biometric identity ID_S.

Step B2: Picks a temporary identity TID_S for *S*.

Step B3: Computers A_S=h (TID_S,K_{HN})$\oplus$$ID_S$, B_S=h (TID_S,ID_S).

Step B4: Picks an identity ID_{IN} for *IN*.

Step B5: Stores the tuple <TID_S,ID_{IN},B_S> in *S*'s memory.

Step B6: Stores the tuple <ID_{IN},$\{TID_S$,$A_S\}_m$ > in *HN*'s memory.

Step B7: Stores the identity ID_{IN} in *IN*'s memory.

3.3 Authentication Phase

Step C1: The sensor node performs as follows:

Acquires a biometric identity ID_S.

Picks a parameter a.

Generates a new timestamp T_1.

Computes C_1=$a$$\oplus$$ID_S$.

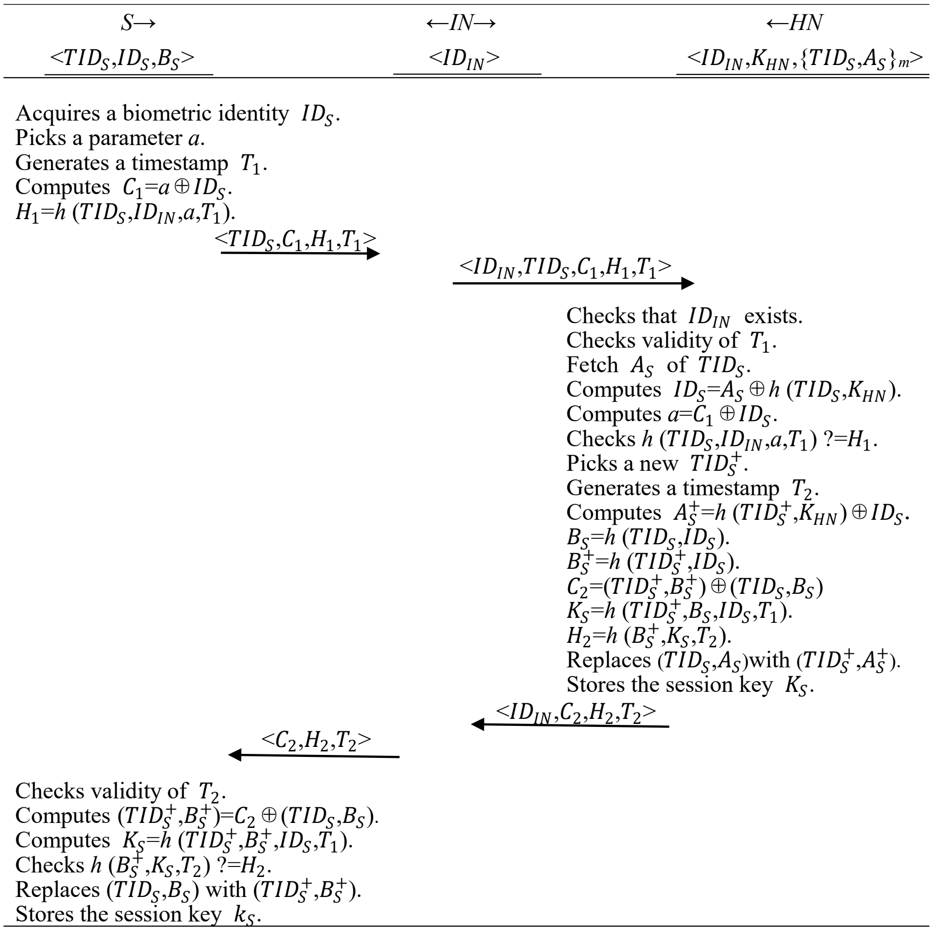
Computes H_1=h (TID_S,ID_{IN},a,T_1).

Sends the tuple <TID_S,C_1,H_1,T_1> to the *IN*.

Step C2: The sensor node performs as follows:

Accepts the tuple <TID_S,C_1,H_1,T_1> from the *SN*.

Sends the tuple <ID_{IN},TID_S,C_1,H_1,T_1> to the *HN*.



S→ <TID_S,ID_S,B_S>

←*IN*→ <ID_{IN}>

←*HN* <ID_{IN},K_{HN},{TID_S,A_S}$_m$>

Acquires a biometric identity ID_S.
Picks a parameter a.
Generates a timestamp T_1.
Computes C_1=$a \oplus ID_S$.
H_1=h (TID_S,ID_{IN},a,T_1).

<TID_S,C_1,H_1,T_1>

<ID_{IN},TID_S,C_1,H_1,T_1>

Checks that ID_{IN} exists.
Checks validity of T_1.
Fetch A_S of TID_S.
Computes ID_S=$A_S \oplus h$ (TID_S,K_{HN}).
Computes a=$C_1 \oplus ID_S$.
Checks h (TID_S,ID_{IN},a,T_1) ?=H_1.
Picks a new TID_S^+.
Generates a timestamp T_2.
Computes A_S^+=h (TID_S^+,K_{HN}) $\oplus ID_S$.
B_S=h (TID_S,ID_S).
B_S^+=h (TID_S^+,ID_S).
C_2=(TID_S^+,B_S^+) $\oplus$ (TID_S,B_S)
K_S=h (TID_S^+,B_S,ID_S,T_1).
H_2=h (B_S^+,K_S,T_2).
Replaces (TID_S,A_S)with (TID_S^+,A_S^+).
Stores the session key K_S.

<ID_{IN},C_2,H_2,T_2>

<C_2,H_2,T_2>

Checks validity of T_2.
Computes (TID_S^+,B_S^+)=$C_2 \oplus$ (TID_S,B_S).
Computes K_S=h (TID_S^+,B_S^+,ID_S,T_1).
Checks h (B_S^+,K_S,T_2) ?=H_2.
Replaces (TID_S,B_S) with (TID_S^+,B_S^+).
Stores the session key k_S.

Figure 2: Authentication phase of our protocol

Step C3: The hub node performs as follows:

Checks that ID_{IN} exists.

Checks validity of T_1.

Fetches A_S of TID_S.

Computes ID_S=$A_S \oplus h$ (TID_S,K_{HN}).

Computes a =$C_1 \oplus ID_S$.

Checks h (TID_S,ID_{IN},a,T_1) ?=H_1.

Picks a new TID_S^+.

Generates a new timestamp T_2.

Computes A_S^+=h (TID_S^+,K_{HN}) $\oplus ID_S$.

Computes B_S=h (TID_S,ID_S).

Computes B_S^+=h (TID_S^+,ID_S).

Computes C_2=(TID_S^+,B_S^+)$\oplus$(TID_S,B_S).

Computes K_S=h (TID_S^+,B_S^+,ID_S,T_1).

Computes H_2=h (B_S^+,K_S,T_2).

Replaces (TID_S,A_S) with (TID_S^+,A_S^+).

Stores the session key K_S.

Sends message <ID_{IN},C_2,H_2,T_2> to the *IN*.

Step C4: The intermediate node performs as follows.

Accepts the tuple <ID_{IN},C_2,H_2,T_2> from the *HN*.

Sends the tuple <C_2,H_2,T_2> to the *SN*.

Step C5: The sensor node performs as follows.

Checks validity of T_2.

Computes (TID_S^+,B_S^+)=$C_2\oplus$(TID_S,B_S).

Computes K_S=h (TID_S^+,B_S^+,ID_S,T_1).

Checks h (B_S^+,K_S,T_2) ?=H_2.

Replaces (TID_S,B_S) with (TID_S^+,B_S^+).

Stores the session key k_S.

The authentication phase of sensor node and hub node is shown in Fig. 2.

4 Informal Security Analysis

In this section, an informal security analysis is conducted to discuss the capability of the proposed protocol to protect against well-known attacks.

4.1 Eavesdropping Attack

The attacker can steal the authentication tuple <TID_S,C_1,H_1,T_1> sent by the sensor node to the hub node, and can steal the authentication element <C_2,H_2,T_2> sent by the hub node to the sensor node. The attacker does not know that the parameter a, as a result of which it cannot calculate the biometric identity ID_S through C_1= $a\oplus ID_S$, nor can it obtain any parameter that can be used to generate the session key K_S. Therefore, the attacker is unable to obtain the session key K_S by launching the eavesdropping attack.

4.2 Anonymous and Untraceable Sessions

The biometric identity ID_S generate a C_1= $a\oplus ID_S$ with a new, random a. XOR operation in each round of conversation. The attacker cannot obtain the biometric identity ID_S, for which the anonymity of the protocol could be ensured. The parameters that comprise the tuple <C_2,H_1,H_2> change in every round of conversation. The attacker is not allowed to connect to the same sensor node in two sessions. Therefore, the protocol of this paper features the anonymity of sensor nodes and the untraceable sessions.

4.3 Sensor Node Capture Attack

The attacker can capture the sensor node and obtain the tuple <TID_S,ID_{IN},B_S> in the memory of the sensor node. But the biometric identity ID_S of the sensor node is unaccessible to the attacker. Therefore, the attacker is unable to obtain the session key K_S through the sensor node capture attack and is thus incapable to pose threat to the security of other sensor nodes.

4.4 Replay Attack

Replay attack is that the attacker resends the message send in the channel to the receiver. Usually timestamps are used to prevent replay attack. In this study, the message sent by S and the message sent by HN contain timestamps T_1 and T_2, respectively. The attacker sends the message stolen in the channel to the receiver again and cannot pass the receiver's timestamp authentication.

4.5 Forward/Backward Security

The session key K_S is protected by a one-way hash function. The parameters that constitute the session key K_S are TID_S, B_S, ID_S and T_1. The biometric identity ID_S is encrypted by a random number a, and the random number a is updated in each round of the session. And there is no correlation between the parameters B_S of different sessions. Thus, the loss of the session key K_S has no impact on the secrecy of previous/future session keys.

5 Performance Analysis

5.1 Storage Cost

In this protocol, each sensor node's memory contains tuple <TID_S,ID_S,B_S>. Each intermediate node's memory contains tuple <ID_{IN}>. Each hub node's memory contains tuple <ID_{IN},K_{HN},$\{TID_S,A_S\}_m$>. The one way hash function used in this protocol is the SHA-256 algorithm, and timestamps $|T_1| = |T_2| = 32$ bits. The length of other parameters are $|TID_S| = |ID_S| = |A_S| = |B_S| = |ID_{IN}| = |K_{HN}| = 256$ bits. Therefore, the sensor node storage cost is 768 bits. The intermediate node storage cost is 256 bits. The hub node storage cost is ($512 + 512m$) bits. The storage consumption of this protocol is shown in the Tab. 2.

Table 2: Storage cost of this protocol

Node	Storage cost (in bits)
SN	768 bits
IN	256 bits
HN	($512 + 512m$) bits

Table 3: Computational cost of this protocol

Node	Computational cost
SN	$3t_h + 2t_{xor} \approx 3t_h$
IN	-
HN	$7t_h + 4t_{xor} \approx 7t_h$

5.2 Computational Cost

The one-way hash function and XOR operation are used in this protocol. We define the computational cost of one way hash function as t_h. XOR operation is less computational cost than one-way hash function and is not considered a computational overhead. In the authentication phase, the total computational cost required for the sensor node and hub node are $3t_h + 2t_{xor} \approx 3t_h$ and $7t_h + 4t_{xor} \approx 7t_h$, respectively. The computational cost of each node is shown in the Tab. 3.

5.3 Communication Cost

The communication cost of the protocol authentication phase is shown in the Tab. 4. In the Step C1, the sensor needs to send tuple <TID_S,C_1,H_1,T_1> = 800 bits of the data to the intermediate node. In the Step C2, the intermediate node need to send tuple <ID_{IN},TID_S,C_1,H_1,T_1> = 1056 bits of the data to the hub node. In the Step C3, the hub node needs to send tuple <ID_{IN},C_2,H_2,T_2> = 800 bits of the data to the intermediate node. In the Step C4, the intermediate node needs to send tuple <C_2,H_2,T_2> = 544 bits of the data to the intermediate node.

Table 4: Communication cost of this protocol

Communication between nodes	Communication cost
$S \rightarrow IN$	800 bits
$IN \rightarrow HN$	1056 bits
$HN \rightarrow IN$	800 bits
$IN \rightarrow S$	544 bits

6 Conclusions

In this paper, a lightweight and secure authentication and key agreement protocol in WBANs is proposed. The protocol involves as few as three hash functions and a small number of XOR operations in the authentication phase, and is characterized by lightweight. The temporary identity mechanism is applied for the sensor nodes, and the temporary identity is updated in each round of the session to ensure the anonymity of the protocol. A large majority of protocols designed for WBANs fail to give considerate to sensor node capture attack. This protocol protects against sensor node capture attack while retaining lightweight and anonymity. Finally, an informal security analysis is conducted to demonstrate how the protocol protects against common attacks.

Funding Statement: This work was supported by the National Natural Science Foundation of China (Grant No. 61872138).

Conflicts of Interest: We declare that we do not have any commercial or associative interest that represents a conflict of interest in connection with the work submitted.

References

[1] W. Liang, M. Tang, J. Long, P. Xin, J. L. Xu *et al.,* “A secure fabric blockchain-based data transmission technique for industrial Internet-of-Things,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3582−3592, 2019.

[2] A. Čolaković and M. Hadžialić, “Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues,” *Computer Networks*, vol. 144, pp. 17−39, 2018.

[3] S. Sarkar, S. Chatterjee and S. Misra, “Assessment of the suitability of fog computing in the context of Internet of Things,” *IEEE Transactions on Cloud Computing*, vol. 6, no. 1, pp. 46−59, 2015.

[4] J. Xu, X. Meng, W. Liang, H. Zhou and K. Li, “A secure mutual authentication scheme of blockchain-based in WBANs,” *China Communications*, vol. 17, no. 9, pp. 34−49, 2020.

[5] R. Negra, I. Jemili and A. Belghith, “Wireless body area networks: Applications and technologies,” *Procedia Computer Science*, vol. 83, pp. 1274−1281, 2016.

[6] Z. Fu, X. Wu, Q. Wang and K. Ren, “Enabling central keyword-based semantic extension search over encrypted outsourced data,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2986−2997, 2017.

[7] K. Li, W. He, Z. Zhang and Q. Zhou, “Node localization for wireless networks in smart distribution automation,” *International Journal of Sensor Networks*, vol. 23, no. 1, pp. 53−60, 2017.

[8] A. M. Koya and P. P. Deepthi, “Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network,” *Computer Networks*, vol. 140, pp. 138−151, 2018.

[9] J. Liu, Z. Zhang, X. Chen and K. S. Kwak, “Certificate less remote anonymous authentication schemes for wireless body area networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 332−342, 2013.

[10] Z. Zhao, “An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem,” *Journal of medical systems*, vol. 38, no. 2, pp. 13−20, 2014.

[11] H. Xiong, “Cost-effective scalable and anonymous certificate less remote authentication protocol,” *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2327−2339, 2014.

[12] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta *et al.,* “Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks,” *Computer Networks*, vol. 129, pp. 429−443, 2017.

[13] A. Gupta, M. Tripathi, T. J. Shaikh and A. Sharma, “A lightweight anonymous user authentication and key establishment scheme for wearable devices,” *Computer Networks*, vol. 149, pp, 29−42, 2019.

[14] Y. Li, Z. Huang, Y. Ma and G. Wen, “acSB: Anti-collision selective-based broadcast protocol in CR-AdHocs,” *Computers, Materials & Continua*, vol. 56, no. 1, pp. 35−46, 2018.

[15] D. Dolev and A. Yao, “On the security of public key protocols,” *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198−208, 1983.