JIST Journal of Information Science and Technology
Volume 11, NO 2 | JUL – DEC 2021 | 29-37
ISSN: 2651-1053 (Online)
ISSN: 1906-9553 (Print)

# Secure Mutual Authentication Protocol Based on Wireless Body Area Networks

*Chalee Thammarat* and Chian Techapanupreeda*

*Faculty of Engineering and Technology, Mahanakorn University of Technology*

Received: October 06, 2021; Revised: December 19, 2021; Accepted: December 23, 2021; Published: December 28, 2021

**ABSTRACT – Data sent from wireless body area networks to healthcare professionals or doctors include sensitive information which needs to be protected from unauthorized access. A mutual authentication protocol is a security feature that can prevent man-in-the-middle and spoofing attacks. A number of mutual authentication protocols based on wireless body area networks have been proposed; however, these impose high cryptographic operation costs, energy costs, and time costs, and also lack some security properties. In this research, we propose an efficient mutual authentication protocol for secure data exchange to send personal health records from a smartphone device to a doctor. The proposed protocol leads to a reduction in the cryptographic operation, energy, and time costs, and uses fewer resources than previous protocols. Although our approach utilizes a one-way hash function rather than encryption, it still provides the necessary security properties, unlike existing protocols. We also formally verify our approach using the Scyther tool and AVISPA. The results show that the proposed protocol has been verified as being resistant to attack as designed.**

**KEYWORDS:** Security, eHealth, Information Security, Scyther, AVISPA, PHRs, PHIs

## 1. Introduction

A personal health record (PHR) contains patient health information needed by health care workers [1]. A PHR may also be used for otherwise healthy people who want to record their health status. The security requirements for PHRs are confidentiality, integrity, and authentication [2, 3], as these protect against threats from attackers seeking to access personal health information, e.g., by altering, eavesdropping on, or denying health information. Many researchers have devised authentication protocols to support all essential aspects of security for wireless body area network (WBAN) data [17-20]. For example, the authors of [17] proposed a key exchange protocol for WBANs that achieved authentication between a control node and a secondary node, between a control node and a primary node, and between a secondary node and a primary node. A timestamp was utilized to guarantee the freshness of the message, and this formed the main security protocol. Their proof of this security protocol used BAN logic. The study in [18]

Introduced a protocol to support selective authentication between nodes and key exchange in a WBAN. This protocol provided the desired security properties, and imposed light computation and communication overheads. In this approach, a random number was adopted instead of a timestamp to reduce the complexity and the cost. The BAN logic model was used to prove this security protocol. The authors of [19] devised a robust anonymous authentication protocol for healthcare applications using a wireless medical sensor network (WMSN). This was suitable for healthcare applications based on a WMSN, and offered strong security and computational efficiency. Both a one-way hash function and symmetric key encryption were applied to ensure the security of the protocol. A formal security analysis was given that used the BAN logic model. In [20], an efficient three-party authentication protocol was suggested for WBANs which used a two-hop star network topology. It made

**Corresponding Author: chalee23@gmail.com*

use of three entities: a central device, a primary node and a secondary node. BAN logic and the AVISPA tool were used to provide a security proof for this protocol.

However, the approaches put forward in [17-20] do not cover all of the necessary security properties, such as mutual authentication, integrity and computational cost. In this paper, we propose a lightweight mutual authentication protocol for WBANs that can maintain the security of sensitive information. It can also be used to solve problems with existing protocols and to overcome their limitations, as a mutual authentication method for a WBAN protocol is still lacking.

This paper is organized as follows. Section 2 discusses some related works. Section 3 presents our proposed protocol, and in Section 4, we analyze the security of our approach. Section 5 compares the performance of our method with existing protocols, and Section 6 concludes the paper and suggests future work.

# 2. Related Works

## 2.1. Wireless Body Area Network (WBAN)

The application and usage of WBANs differ depending on which devices are used [4, 6-8]. For medical applications, they can provide valuable information monitoring via wireless communication [5], such as data from electrocardiogram (ECG), heart rate, or blood pressure sensors. Many researchers have presented protocols for medical body area networks. For instance, the authors of [9] designed a protocol based on lightweight identity-based encryption, to provide security and privacy for a body sensor network. In [10], a secure healthcare system for IoT was proposed, based on elliptic curve cryptography (ECC). Both of these approaches used strong encryption that consumed considerable computational resources but was suitable for body sensor networks and healthcare applications. As mentioned above, the security requirements for sending PHR data via a network are confidentiality, integrity, and authentication. Consequently, when sending PHRs via WBAN devices, these security requirements require consideration.

## 2.2. IEEE 802.15 Security

The security of body area networks relies on IEEE 802.15, and in this research, we will focus only on IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (ZigBee), and IEEE 802.15.6 Task Group 6 (TG6), which are described below.

2.2.1. The IEEE 802.15 Task Group 6 is developing a communication standard that is optimized for low-power devices for operation on, in or around the human body (not limited to humans), to serve a variety of applications including medical, consumer electronics, and personal entertainment. The security of TG6 supports confidentiality, integrity and authentication but does not consider authorization and non-repudiation of the message. It is optimized for low-power devices and operation with the human body, i.e., for smartwatches or blood pressure tags [11].

2.2.2. Bluetooth (IEEE 802.15.1) is a wireless technology band at 2.4 GHz. The security of Bluetooth supports only two security properties, confidentiality and authentication, and is not applicable to body area networks. The reader can find more information on Bluetooth in [12].

2.2.3. ZigBee (IEEE 802.15.4) can be applied to create a personal area network, in which symmetric key encryption is used to secure the communication between devices. However, Zigbee supports only two security properties, which are confidentiality and authentication [13].

# 3. Proposed Protocol

In this section, we propose a mutual authentication protocol for a WBAN. Our protocol provides mutual authentication between *P* and *AGW*, and between *D* and *AGW*. The details of the mutual authentication process are explained below.

## 3.1. Notation

Our proposed protocol uses the symbols and notation given in Table 1.

*Table 1. Notation used in the proposed protocol.*

| Symbol | Definition |
|---|---|
| $P$ | A smartphone of a patient who owns personal health information |
| $D$ | Doctors, hospital, professional care or clinical |
| $AGW$ | Authentication gateway |
| $P_{ID}$ | The identity of a patient |
| $D_{ID}$ | The identity of the infirmary |

| Symbol | Definition |
|---|---|
| $SK_{A\text{-}B}$ | Symmetric key between party *A* and party *B* |
| $\{M\}_{SKA\text{-}B}$ | A message encrypted with a symmetric key between party *A* and party *B* |
| *h(M)* | Hash function of message *M* |
| $N_A$ | A nonce is issued by party *A* |
| $T_A$ | Current timestamp created by party *A* |

## 3.2. Network Model

Our network model includes body sensors and the *P, D* and *AGW* entities, as shown in Figure 1. The body sensors need to be verified, and are resource-limited devices. *P* acts as an intermediate node between the body sensors and *AGW*, and has more resources than the body sensors. It is usually a portable device such as a smartphone, tablet or notebook. *AGW* is rich in resources (i.e., has more resources than *P*), and is usually a server. We assume that the communication between all entities is flexible.

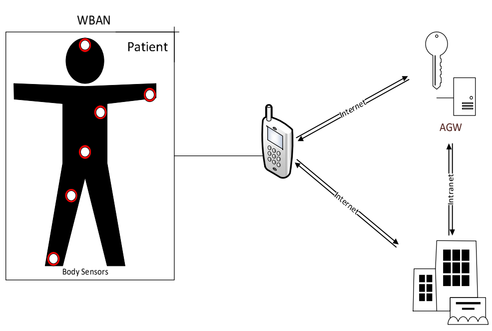


*Figure 1. Network model of the proposed protocol.*

## 3.3. Registration

In the registration phase, *P* and *D* register with *AGW* to share the key between *P* and *AGW*, and between *D* and *AGW*. Registration is performed via a secure channel.

3.3.1. Registration of *P* with *AGW*

*P* connects to *AGW* via a secure communication channel, and sends a request to *AGW*. When *AGW* receives this request, it generates $P_{ID}$ and the key $SK_{P\text{-}AGW}$ and sends these back to *P*. Note that $SK_{P\text{-}AGW}$ is shared between *P* and *AGW*.

3.3.2. Registration of *D* with *AGW*

*D* connects with *AGW* via a secure communication channel, and sends a request to *AGW*. When *AGW* receives this request, it generates $D_{ID}$ and the key $SK_{D\text{-}AGW}$ and sends these back to *D*. Note that $SK_{D\text{-}AGW}$ is shared between *D* and *AGW*.

## 3.3. Mutual Authentication Protocol

We propose a protocol to prevent misuse of patient health information and to protect against threats. A smartphone is used to read and check the sensors on the patient's body, such as blood pressure monitors. If the blood pressure (BPI) is equal to or more than 140SYS/90DIA mm *HG*, the smartphone sends the patient's identity to the emergency medical services (as an emergency case). In this case, the system sends $P_{ID}$, $D_{ID}$, and BPI directly to the emergency medical service (EMS) and calls for help. This because hypertension may threaten a patient's life, by causing a heart attack, stroke, or aneurysm. The patient therefore needs immediate treatment in order to save their life.

In contrast, if a patient's BPI is in the normal range, the system sends information to the devices when it needs a doctor or hospital to retrieve it directly when needed. The details of the proposed protocol are set out below.

**M1: D→AGW:** $D_{ID}, P_{ID}, N_D, T_D, h(D_{ID}, P_{ID}, N_D, T_D, SK_{D\text{-}AGW})$

**M2: AGW→P:** $D_{ID}, P_{ID}, N_D, T_D, h(D_{ID}, P_{ID}, N_D, T_D, SK_{D\text{-}AGW}), h(D_{ID}, P_{ID}, N_D, T_D, h(D_{ID}, P_{ID}, N_D, T_D, SK_{D\text{-}AGW}), SK_{P\text{-}AGW}))$

**M3: P→AGW:** $N_P, h(N_P, h(D_{ID}, P_{ID}, N_D, T_D, h(D_{ID}, P_{ID}, N_D, T_D, SK_{D\text{-}AGW}), SK_{P\text{-}AGW}), SK_{P\text{-}AGW})$

**M4: AGW→P:** $N_{AGW}, T_{AGW}, \{SK_{P\text{-}D}, h(D_{ID}, P_{ID}, N_D, N_P, N_{AGW}, T_D, T_{AGW}, SK_{P\text{-}D}, SK_{P\text{-}AGW})\}_{SKP\text{-}AGW}$

**M5: AGW→D:** $N_{AGW}, T_{AGW}, \{SK_{P\text{-}D}, h(D_{ID}, P_{ID}, N_D, N_P, N_{AGW}, T_D, T_{AGW}, SK_{P\text{-}D}, SK_{D\text{-}AGW})\}_{SKD\text{-}AGW}$

In message M1, *D* sends $D_{ID}, P_{ID}, N_D, T_D, h(D_{ID}, P_{ID}, N_D, T_D, SK_{D\text{-}AGW})$ to *AGW* to request a connection with *P*. After receiving message M1 from *D, AGW* uses $D_{ID}$, $P_{ID}$, $N_D$, $T_D$ and $SK_{D\text{-}AGW}$

to compute the hash value and compares it with $h(D_{ID}, P_{ID}, N_D, T_D, SK_{D\text{-}AGW})$. If the two hash values are equal, *AGW* will continue with M2; otherwise, it terminates the connection. Note that the message contains $h(D_{ID}, P_{ID}, N_D, T_D, SK_{D\text{-}AGW})$ and is considered a message authentication code (MAC) that can ensure the integrity of the message.

After verifying that *D* is the originator of the message, *AGW* will send $D_{ID}, P_{ID}, N_D, T_D, h(D_{ID}, P_{ID}, N_D, T_D, SK_{D\text{-}AGW}), h(D_{ID}, P_{ID}, N_D, T_D, h(D_{ID}, P_{ID}, N_D, T_D, SK_{D\text{-}AGW}), SK_{P\text{-}AGW}))$ to *P* in message M2. This message can be used to ensure that *AGW* is the sender, since *AGW* possesses both the symmetric key $SK_{D\text{-}AGW}$ and $SK_{P\text{-}AGW}$. Once *P* has received message M2 from *AGW*, it will check the correctness of the message by checking the hash value of $D_{ID}, P_{ID}, N_D, T_D, h(D_{ID}, P_{ID}, N_D, T_D, SK_{D\text{-}AGW}), h(D_{ID}, P_{ID}, N_D, T_D, h(D_{ID}, P_{ID}, N_D, T_D, SK_{D\text{-}AGW}), SK_{P\text{-}AGW}))$. If this is correct, *P* sends $N_P, h(N_P, h(D_{ID}, P_{ID}, N_D, T_D, h(D_{ID}, P_{ID}, N_D, T_D, SK_{D\text{-}AGW}), SK_{P\text{-}AGW}), SK_{P\text{-}AGW})$ to *AGW* in message M3. Otherwise, *P* terminates the connection.

When *AGW* has received message M3 and has checked that the message was sent from *P*, it will send a nonce, the timestamp of *AGW*, the shared $SK_{P\text{-}D}$ key and $h(D_{ID}, P_{ID}, N_D, N_P, N_{AGW}, T_D, T_{AGW}, SK_{P\text{-}D}, SK_{P\text{-}AGW})$, encrypted with $SK_{P\text{-}AGW}$, to *P* in message M4.

*AGW* then sends a nonce, the timestamp of *AGW*, the shared $SK_{P\text{-}D}$ *key* and $h(D_{ID}, P_{ID}, N_D, N_P, N_{AGW}, T_D, T_{AGW}, SK_{P\text{-}D}, SK_{P\text{-}AGW})$, encrypted with $SK_{D\text{-}AGW}$, to *D* in message M5. The goal of this step is to send the shared symmetric key $SK_{P\text{-}D}$ to *P* and *D* to allow them to exchange personal health information via a secure channel.

It can be seen that the proposed protocol ensures mutual authentication between *P* and *AGW*, and between *D* and *AGW*. Each message in the proposed protocol can be used to identify the sender of the original message. We use only symmetric cryptographic operations, a MAC and a hash function to provide mutual authentication, and this results in lightweight protocol that is suitable for a WBAN.

# 4. Security Analysis

## 4.1. Informal Security Analysis

In this section, we present a security analysis of the proposed protocol to prove that it provides the necessary security, as follows:

4.1.1. Mutual authentication: This is an important security property that is used to identify the sender and the receiver of the messages. The proposed protocol deploys a MAC to provide mutual authentication between entities, which can expressed as in the message below:

**M2: AGW→P:** $D_{ID}, P_{ID}, N_D, T_D, h(D_{ID}, P_{ID}, N_D, T_D, SK_{D\text{-}AGW}), h(D_{ID}, P_{ID}, N_D, T_D, h(D_{ID}, P_{ID}, N_D, T_D, SK_{D\text{-}AGW}), SK_{P\text{-}AGW}))$

*AGW* cannot deny sending the original message to *P*, as only *AGW* possesses both the symmetric keys $SK_{D\text{-}AGW}$ and $SK_{P\text{-}AGW}$. Hence, only *AGW* can construct this message or the original message.

**M5: AGW→D:** $N_{AGW}, T_{AGW}, \{SK_{P\text{-}D}, h(D_{ID}, P_{ID}, N_D, N_P, N_{AGW}, T_D, T_{AGW}, SK_{P\text{-}D}, SK_{D\text{-}AGW})\}_{SKD\text{-}AGW}$

*AGW* cannot deny sending the original message to *D*, as only *AGW* possesses both the symmetric keys $SK_{D\text{-}AGW}$ and $SK_{P\text{-}D}$. Hence, only *AGW* can construct this message or the original message.

4.1.2. Integrity: This property ensures at the recipient's end that the information in the received message has not been altered by an attacker during the exchange of messages. The proposed protocol utilizes a cryptographic hash function and a MAC to guarantee message integrity.

4.1.3. Confidentiality: Personal health information should not made be available or disclosed to unauthorized persons, and should be protected from disclosure to an attacker. Health information should be confidential, and made available only to authorized doctors. The proposed protocol applies a symmetric key to encrypt the messages that are exchanged between parties. This can ensure that the protocol provides message confidentiality.

4.1.4. Replay attack: In this scenario, an attacker records old messages and then resends them, as these are valid message transmissions. The attacker therefore gets the same messages as the legitimate parties. The proposed protocol uses a nonce and a timestamp at each step of the protocol, which can prevent replay attacks.

4.1.5. Eavesdropping attack: In this case, an attacker secretly listens to a conversation transmitted over the air between parties, to obtain medical information about the victim. The goal of the attacker is to learn the content of the exchanged message. An attacker that eavesdrops on medical information can collect a large amount of information. To prevent this, the proposed protocol uses symmetric key encryption for the message exchange.

4.1.6. Data modification: An attacker could edit a message and send it on to the receiver during the communication process, which could result in a false diagnosis. Data modification cannot occur in our scheme, since we use symmetric cryptography, including a hash function, in each step.

4.1.7. MITM attack: An attacker cannot analyze a transmitted message or fraudulently pose as one of the parties (i.e., the sender or receiver), since the proposed protocol uses a cryptographic hash function and symmetric key cryptography to maintain the confidentiality of messages and the message integrity. Furthermore, our protocol applies a MAC to identify the sender and the receiver, who share the same symmetric keys.

From Table 2, it can be seen that scheme in [19] and our approach provide all of the security properties, whereas the protocols in [17, 18, 20] do not ensure message integrity.

*Table 2. Security comparison of the proposed protocol and existing alternatives.*

| | [17] | [18] | [19] | [20] | P |
|---|---|---|---|---|---|
| Mutual authentication | N | Y | Y | Y | Y |
| Integrity | N | N | Y | N | Y |
| Confidentiality | Y | Y | Y | Y | Y |
| Replay attack | Y | Y | Y | Y | Y |
| Eavesdropping attack | Y | Y | Y | Y | Y |
| Data Modification | Y | Y | Y | Y | Y |
| Man-in-the-middle attack | Y | Y | Y | Y | Y |

P: Our protocol

## 4.2. Formal Security Analysis

4.2.1. Using Scyther

We used the Scyther tool to verify that our proposed protocol was safe and robust against attacks. Security Protocol Description Language (SPDL) code for the proposed protocol is shown in Figures 2, 3 and 4, we present the results of verification, claims and automatic claims of the proposed protocol that has no attack. More information about Scyther can be found in [14, 15].

```
/* Mutual Authentication Protocol */
hashfunction h;
usertype Timestamp;
const DiD, PiD;
const SKP-AGW, SKD-AGW, SKP-D
    :SessionKey;
macro m1 = DiD, PiD, nd, td, h(DiD, PiD,
    nd, td, SKD-AGW);
macro m2 = DiD, PiD, nd, td, h(DiD, PiD,
    nd, td, SKD-AGW), h(DiD, PiD, nd, td,
    h(DiD, PiD, nd, td, SKD-AGW, SKP-
    AGW));
macro m3 = np, h(np, h(DiD, PiD, nd, td,
    h(DiD, PiD, nd, td, SKD-AGW), SKP-
    AGW, SKP-AGW));
macro m4 = nagw, tagw,{SKP-D, h(DiD,
    PiD, nd, np, nagw, td, tagw, SKP-D, SKP-
    AGW)}SKP-AGW;
macro m5 = nagw, tagw, {SKP-D, h(DiD,
    PiD, nd, np, nagw, td, tagw, SKP-D,
    SKD-AGW)}SKD-AGW;
// The protocol description
protocol M-Auth(D, AGW, P)
{
role D
```

```
{
fresh td, tagw: Timestamp;
fresh nr, ni, nd, np, nagw: Nonce;
send_1(D, AGW, m1);
recv_5(AGW, D, m5);
claim_d1(D, Secret, nd);
claim_d2(D, Secret, np);
claim_d3(D, Alive);
claim_d4(D, Weakagree);
claim_d5(D, Commit, AGW, nd,np);
claim_d6(D, Niagree);
claim_d7(D, Nisynch);
}
role AGW
{
fresh nr, ni, nd, np, nagw: Nonce;
fresh td, tagw: Timestamp;
recv_1(D, AGW, m1);
send_2(AGW, P, m2);
recv_3(P, AGW, m3);
send_4(AGW, P, m4);
send_5(AGW, D, m5);
claim_agw1(AGW, Secret, nagw);
claim_agw2(AGW, Secret, tagw);
claim_agw3(AGW, Alive);
claim_agw4(AGW, Weakagree);
claim_agw5(AGW, Commit, P, nagw);
claim_agw6(AGW, Niagree);
claim_agw7(AGW, Nisynch);
claim_agw8(AGW, Commit, D, nagw);
}
role P
{
fresh nr, ni, nd, np, nagw : Nonce;
fresh td, tagw: Timestamp;
recv_2(AGW, P, m2);
send_3(P, AGW, m3);
recv_4(AGW, P, m4);
claim_P1(P, Secret, nagw);
claim_P2(P, Secret, np);
claim_p3(P, Alive);
claim_p4(P, Weakagree);
claim_p5(P, Commit, D, np,nagw);
claim_p6(P, Niagree);
claim_p7(P, Nisynch);
}
/* End of Program */
}
```

*Figure 2. SPDL code for the proposed protocol.*


*Figure 3. Verification results from the Scyther tool.*


*Figure 4. Autoverification using the Scyther tool.*

4.2.2. Using AVISPA

We also used AVISPA to prove that our proposed protocol is safe and is robust against attacks. There are numerous research papers that have applied this approach to prove their protocols [21, 22]. AVISPA uses the High-Level Protocol Specification Language (HLPSL) specification syntax to generate a graphical on-the-fly model checker (OMFC), constraint-logic-based model checker (ATSE), and attack trace generation, to determine whether or not the authentication protocol is vulnerable to attack. The results from OMFC, ATSE and attack generation are shown in Figures 5 and 6.

*Figure 5. OMFC results verified using AVISPA.*

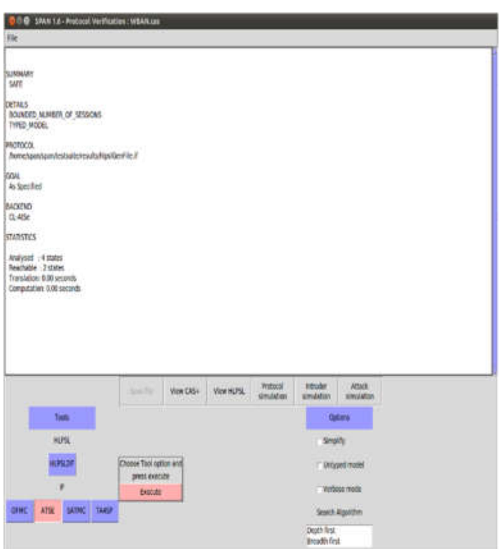

*Figure 6. ATSE results verified using AVISPA.*

# 5. Performance Analysis

Tables 3 to 5 and Figures 7 to 9 show the results for cryptographic operations cost, energy cost and time cost, respectively, and provide a comparison with the protocols in [17-20]. It can be seen that our protocol imposes lower cryptographic operations, energy and time costs than the protocols in [17-20]. Note that the process used to measure the energy consumption is derived from [23], and the method used to measure the time consumption is derived from [24]. Note that symmetric encryption uses the Advanced Encryption Standard (AES) while a one-way hash function uses Secure Hashing Algorithm (SHA1). P stands for the proposed protocol.

*Table 3. Comparison of cryptographic operation cost.*

| | AES | SHA1 | Total |
|---|---|---|---|
| [17] | 7 | 0 | 7 |
| [18] | 6 | 0 | 6 |
| [19] | 5 | 2 | 7 |
| [20] | 6 | 0 | 6 |
| P | 2 | 5 | 7 |


*Figure 7. Comparison of cryptographic operation cost.*

*Table 4. Comparison of energy consumption.*

| | **AES (1.21 µJ/byte)** | **SHA1 (0.76 µJ/byte)** | **Total** |
|---|---|---|---|
| [17] | 8.47 | 0 | 8.47 |
| [18] | 7.26 | 0 | 7.26 |
| [19] | 6.05 | 1.52 | 7.57 |
| [20] | 7.26 | 0 | 7.26 |
| P | 2.42 | 3.8 | 6.22 |

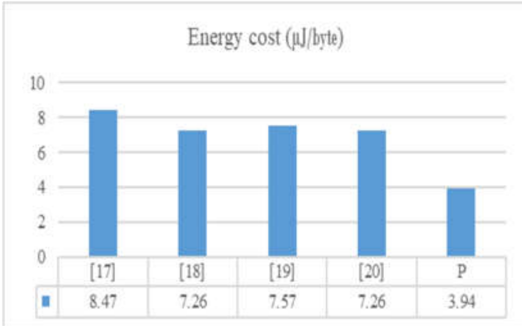


*Figure 8. Comparison of energy consumption.*

*Table 5. Comparison of time consumption.*

| | AES (1.71 ms/byte) | SHA1 (1.28 ms/byte) | Total |
|---|---|---|---|
| [17] | 11.97 | 0 | 11.97 |
| [18] | 10.26 | 0 | 10.26 |
| [19] | 8.55 | 2.56 | 11.11 |
| [20] | 10.26 | 0 | 10.26 |
| P | 3.42 | 6.4 | 9.82 |

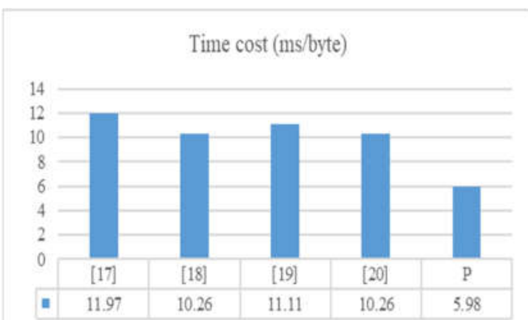


*Figure 9. Comparison of time consumption.*

## 6. Conclusion and Discussion

Protocol for WBAN devices needs to provide all essential security properties, to protect against misuse of patient health information and prevent threats from attackers. We have analyzed the security of our proposed protocol and compared it with other existing alternatives. The results of our analysis show that the proposed protocol provides security properties such as mutual authentication, integrity, confidentiality, and protection against replay, eavesdropping, data modification and MITM attacks. Our cryptographic algorithms use only symmetric encryption and a hash function, which enhances security while creating a lightweight protocol that is more effective than other protocols. The results from the Scyther tool show that our proposed protocol ensures the most important security properties needed for a WBAN and is robust against attackers.

In future work, we will focus on developing a prototype based on the proposed protocol, in order to show that our approach is practical for real- world applications.

## References

[1] C. Techapanupreed, W. Kurutach, "Enhancing transaction security for handling accountability in electronic health records," Security and Communication Networks, 2020.

[2] G. hamilarasu, and A. Odesile, "Securing wireless body area networks: Challenges, review and recommendations," International Conference on Computational Intelligence and Computing Research (ICCIC), pp. 1-7, 2016.

[3] M. Kompara, and M. Hölbl, "Survey on security in intra-body area network communication," Ad Hoc Networks, vol. 70, pp. 23-43, 2018.

[4] D. Vera, N. Costa, L. Roda-Sanchez, T. Olivares, A. Fernández-Caballero, and A. Pereira, "Body area networks in healthcare: A brief state of the art," Applied Sciences, vol. 9, no. 16, pp. 3248, 2019.

[5] F. R. Yazdi, M. Hosseinzadeh, and S. Jabbehdari, "A review of state-of-the-art on wireless body area networks," International Journal of Advanced Computer Science and Applications, pp. 443-455, 2017.

[6] R. A. Khan, and A. S. K. Pathan, "The state-of-the-art wireless body area sensor networks: A survey," International Journal of Distributed Sensor Networks, vol. 14, no. 4, 2018.

[7] C. A. Tavera, J. H. Ortiz, O. I. Khalaf, D. F. Saavedra, and T. H. Aldhyani, "Wearable wireless body area networks for medical applications," Computational and Mathematical Methods in Medicine, 2021.

[8] S. J. Hussain, M. Irfan, N. Z. Jhanjhi, K. Hussain, and M. Humayun, "Performance enhancement in wireless body area networks with secure communication," Wireless Personal Communications, vol. 116, no. 1, pp. 1-22, 2021.

[9] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "Body sensor network security: an identity-based cryptography approach," In Proceedings of the first ACM conference on Wireless network security, pp. 148-153, 2008.
[10] K. H. Yeh, "A secure IoT-based healthcare system with body sensor networks," IEEE Access, vol. 4, pp. 10288-10299, 2016.
[11] IEEE 802.15 WPAN Task Group 6 (TG6) Body Area Networks". IEEE Standards Association. 9 Jun 2011. Retrieved 9 Dec 2021.
[12] IEEE Standard for Information technology-- Local and metropolitan area networks- "Specific requirements-- Part 15.1a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN)," in IEEE Std 802.15.1-2005 (Revision of IEEE Std 802.15.1-2002) , vol., no., pp.1-700, 14 June 2005, doi: 10.1109/IEEESTD.2005.96290.
[13] Approved IEEE Draft Amendment to IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Part 15.4: "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANS): Amendment to Add Alternate Phy (Amendment of IEEE Std 802.15.4)," in IEEE Approved Std P802.15.4a/D7, Jan 2007 , 2007.
[14] C. J. Cremers, "The Scyther tool: Verification, falsification, and analysis of security protocols," In International Conference on Computer Aided Verification, Springer, Berlin, Heidelberg, pp. 414-418, 2008.
[15] C. Thammarat, and W. Kurutach, "A lightweight and secure NFC-base mobile payment protocol ensuring fair exchange based on a hybrid encryption algorithm with formal verification," International Journal of Communication Systems, vol. 32, no. 12, 2019.
[16] W. Stallings, L. Brown, , M. D. Bauer, and A. K. Bhattacharjee, "Computer security: principles and practice," Upper Saddle River, NJ, USA: Pearson Education, pp. 978, 2012.
[17] R. Yan, J. Liu, and R. Sun, "An efficient authenticated key exchange protocol for wireless body area network," The Proceedings of the Third International Conference on Communications, Signal Processing, and Systems, Springer, Cham, pp. 51-58, 2015.
[18] J. Liu, Q. Li, R. Yan, and R. Sun, "Efficient authenticated key exchange protocols for wireless body area networks," EURASIP Journal on Wireless Communications and Networking, pp. 1-11, 2015.
[19] D. He, N. Kumar, J. Chen, C. C. Lee, N. Chilamkurti, and S. S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," Multimedia Systems, vol. 21, no. 1, pp. 49-60, 2015.
[20] R. Vishwakarma, and R. K. Mohapatra, "A secure three-party authentication protocol for wireless body area networks," In 2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS), pp. 99-103, 2017.
[21] C. Thammarat, and C. Techapanupreeda, "A secure authentication and key exchange protocol for M2M communication," In 2021 9th International Electrical Engineering Congress (iEECON), pp. 456-459, IEEE, 2021.
[22] C. Thammarat, and C. Techapanupreeda, "A secure mobile payment protocol for handling accountability with formal verification," In 2021 International Conference on Information Networking (ICOIN), pp. 249-254, IEEE, 2021.
[23] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," in IEEE Trans. Mobile computing, vol. 5, no. 2, pp. 128-143, 2006.
[24] X. Zheng, L. Yang, J. Ma, G. Shi, and D. Meng, "TrustPAY: Trusted mobile payment on security enhanced ARM TrustZone platforms," in Proc. on Computers and Communication, pp. 456-462, 2016.