Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 6370742, 11 pages
https://doi.org/10.1155/2019/6370742

Research Article

SUBBASE: An Authentication Scheme for Wireless Sensor Networks Based on User Biometrics

Rabia Riaz,[1] Noor-ul-Ain Gillani,[1] SanamShahla Rizvi,[2] Sana Shokat,[1] and Se Jin Kwon[3]

[1]*Department of CS & IT, University of Azad Jammu and Kashmir, Muzaffarabad 42714, Pakistan*
[2]*Raptor Interactive (Pty) Ltd., Eco Boulevard, Witch Hazel Ave, Centurion 0157, South Africa*
[3]*Department of Computer Engineering, Kangwon National University, Samcheok 25806, Republic of Korea*

Correspondence should be addressed to Se Jin Kwon; sjkwon@kangwon.ac.kr

Received 9 November 2018; Revised 6 February 2019; Accepted 13 March 2019; Published 4 April 2019

Guest Editor: Fawad Zaman

To keep a network secure, a user authentication scheme that allows only authenticated users to access network services is required. However, the limited resources of sensor nodes make providing authentication a challenging task. We therefore propose a new method of security for a wireless sensor network (WSN). Our technique, Secure User Biometric Based Authentication Scheme (SUBBASe), is based on the user biometrics for WSNs. It achieves a higher security level as well as improved network performance. This solution consists of easy operations and light computations. Herein, the proposed technique is evaluated and compared with previous existing techniques. This scheme increases the performance of the network by reducing network traffic, defending against DOS attacks, and increasing the battery life of a node. Consequently, the functionality and performance of the entire network is improved.

1. Introduction

Wireless sensor networks (WSNs) contain sensor nodes for specific purposes [1]. Tiny sensor nodes in the network process information they receive after sensing their surroundings. Such networks can be applied to a large number of applications including structural health monitoring, environmental control, and battlefield surveillance [2]. In most of these applications, the user can receive data directly through a gateway node because requests are processed on this node. However, receiving data from a gateway node is occasionally difficult or even impossible. Therefore, data are obtained directly through sensor nodes [3]. Sensed data may be confidential, and illegal users can easily access sensitive data by sending a request to a sensor node. Because it is difficult for a sensor node to authenticate a request message, the leakage of sensitive information and an unnecessary depletion of network resources, e.g., node power and network bandwidth, may occur. Each of the above problems can affect the lifetime and performance of the network and make the system unattainable for legitimate users. Thus, user authentication is a required service to resist the illegal use of network data and resources [4]. To accomplish this, it is very important for sensor nodes to authenticate the identities of users. User authentication is a final solution to each of the above problems and allows authenticated users to join a network. Unfortunately it is a tremendously challenging task to provide authentication in WSNs owing to the resource limitation of its tiny sensor devices, i.e., energy and memory limitations, as well as their computational and communicational capabilities. Although various protocols have been proposed, their authentication process remains insecure [5–7]. Ultimately, to ensure the safety of a WSN, a protocol that utilizes a stronger and smarter mechanism is needed.

In this paper, we offer a competent user authentication technique for WSN applications. This scheme overcomes the authentication problem and improves the effectiveness of WSNs. We propose an authentication scheme called the Secure User Biometric Based Authentication Scheme (SUBBASe). The purposes of the designed authentication mechanism are as follows:

(i) increase the network performance by reducing network traffic;

(ii) save the battery power of the nodes, thus enhancing the lifetime of the WSN; and

(iii) defend the sensor network against different types of attacks, thus improving the functionality and performance of the entire network.

The remainder of this paper is organized as follows: Section 2 discusses the user authentication problems in existing WSN schemes through a step-by-step approach. In Section 3, we describe our proposed biometric-based user authentication protocol. Section 4 provides the security aspects of the proposed security protocol. Section 5 presents the proof of significance of SUBBASE using BAN Logic. Section 6 analyzes the performance of proposed protocol based on analytical modeling. Finally, Section 7 gives concluding remarks regarding this research.

2. Literature Review

Wong et al. [8] proposed a user authentication scheme based on the user password and cryptographic hash functions. This scheme is vulnerable to various security attacks such as forged, replay, and stolen-verifier attacks. Because a gateway and login node maintains tables containing registered user information, user passwords may be exposed by any of the sensor nodes, and a user may be blocked from altering their password [19].

Das et al. [9] proposed a user authentication scheme for a WSN that overcomes the security flaws of the scheme proposed by Wong et al. [8]. This scheme is based on the use of a smart card and the user's password. Although this scheme overcomes the weaknesses of Wong et al.'s scheme, it suffers from several security threats. For a data transmission, for example, no secure medium is provided and thus an attacker can easily alter the transmitted data. In addition, this protocol is not robust because its robustness depends on a secret parameter that is preinstalled in the sensor nodes and smart cards. If a node is captured or compromised, the security of the entire network will be harmed. In addition, an attacker can overhear entire conversation of all entities on a network. A compromised node is a major problem in this scheme and is defenseless against various types of attacks such as replaying, impersonation, password guessing, and DOS attacks.

Khan and Alghathbar [10] showed that the scheme proposed by Das et al. [9] does not provide mutual authentication and is defenseless against privileged insider attack. They determined that it is not possible to freely change a password with Das et al.'s scheme. Thus, Khan and Alghathbar proposed a security technique that attempts to overcome all of these security flaws. Using their proposed protocol, they added a user-password changing phase to Das et al.'s scheme to allow users to easily change their password. Whenever any user wishes to amend a password, the smart card overwrites the old password with a new one. To overcome the existing problems in Das et al.'s scheme, the approach proposed by Khan and Alghathbar is based on the hashed value of plain text, namely, a password. In Das et al.'s scheme, a simple password without the use of a hash value is sent to the gateway node, which causes various insider attacks to occur in a network. Thus, the hash value of the password decreases the probability of an insider attack in a network. To a certain extent, their proposed work offers security to a network by reducing the flaws in Das et al.'s scheme; however, this proposed scheme also has certain security flaws. For example, there is a problem of a session key not being established between two entities, namely, the sensor node and user, and thus mutual authentication is not provided and the problem of a lack of confidentiality of messages transmitted between participants may occur.

Yuan et al. [11] offered a protocol based on the biometrics of the user. A password and smart card are used in this particular approach. Transmitted data are not encrypted, and if an unauthorized user captures any sensor nodes, the unauthorized user can easily view the messages. Moreover, an attacker can exchange messages as a legal entity between a sensor node and user and finally gather all information available. In addition, no secure channel is provided, making message confidentiality and data integrity major problems with this particular scheme.

Yoon et al. [12] proposed an enhancement of Yuan et al.'s protocol [11] that is based on biometrics but without the use of a password. With this protocol, two secret parameters are used. Through these secret parameters, each entity verifies the legitimacy of all other entities in the network. Data integrity is considered with this protocol. However, this scheme still has security flaws because the response message of the user sent by the sensor node is not encrypted, and therefore a confidentiality problem still exists. The protocol also faces various types of DOS attacks.

To overcome the flaws to Yoon et al.'s protocol, Debiao [13] introduced another protocol based on the user's biometrics. This protocol requires complicated hardware and consumes too much time and energy. Also their protocol was vulnerable to various types of attacks, such as DOS, guessing, and replay attacks [20]. Kaul et al. [14] proposed a smart card and password-based user authentication scheme. It provides no security for user identity. It is susceptible to offline password guessing attack and smart card stolen attack and session key compromise attacks are possible. SungJin et al. [15] proposed a smart card based authentication protocol for wireless sensor network in vehicular communication.

Node compromise, message confidentiality, and data integrity are major problems with existing protocols, which also require complicated hardware. The security of previous user authentication security protocols is based on the application of a password. Short passwords are easily broken with the help of a password guessing attack. In addition, a user's password can be shared with other people or can be stolen, and there is no technique to determine an actual user. Similarly, other authentication protocols require special hardware support.

Therefore, biometric authentication is an ultimate solution to such security problems [21] and is more secure and reliable than conventional password-based authentication. Althobaiti et al. [16] pointed out numerous types of security vulnerabilities in traditional user authentication protocols

Table 1: Summary of previous authentication techniques.

Protocols	Man in the middle attack	Guessing attack	Insider attack	Replay attack	Data Integrity provided	Biometric Based	Smart Card Based
Wong [8]	Insecure	Insecure	Insecure	Insecure	No	No	No
Das and Ambani [9]	Insecure	Insecure	Insecure	Insecure	No	No	Yes
Khan and Alghathbar [10]	Insecure	Insecure	Secure	Secure	Yes	No	Yes
Yaun [11]	Insecure	Secure	Insecure	Secure	No	Yes	Yes
Yoon [12]	Insecure	Secure	Insecure	Secure	Yes	Yes	Yes
Debiao [13]	Insecure	Secure	Secure	Secure	Yes	Yes	Yes
Kaul [14]	Insecure	Insecure	Secure	Secure	No	No	Yes
SungJin [15]	Secure	Secure	Secure	Secure	Yes	No	Yes
Althobaiti [16]	Insecure	Secure	Secure	Secure	Yes	Yes	No
Dongwoo [17]	Secure	Secure	Secure	Secure	Yes	Yes	Yes
BAS [18]	Secure	Secure	Insecure	Secure	Yes	No	No

and proposed an efficient biometric-based user authentication scheme for WSNs. This scheme is feasible for resource constrained devices because it is based on a hash function and biometric encryption without the use of any complicated equipment.

Dongwoo et al. [17] removed the shortcomings of Kaul at el. [14] and proposed a more secure user authenticated key agreement method. They use user biometric based Biohash function for user authentications. Their analysis showed that their scheme is robust against all the attacks that Kaul at el. scheme was susceptible to and additionally it provides the high level of security without the requirements of time synchronization.

For authentications in sensor networks, Bi-Phase Authentication Scheme (BAS) is presented by Rabia at el. [18]. This scheme provides initial small scale authentication of the request messages entering in wireless sensor networks and provides resistance against DOS attack.

Although all of the above schemes and many other recent schemes [22–24] have suggested security improvements, there still remain drawbacks with regard to their protocols, as summarized in Table 1, such that a session key is not established after user authentication and message confidentiality is not considered. In addition, these protocols require extra hardware and are vulnerable to different types of DOS attacks. Our proposed protocol fulfills the above-mentioned shortcomings and increases the security of user authentication in a WSN.

3. Proposed User Biometric Based Secure Authentication Scheme

Owing to the exceptional characteristics of fingerprint authentication as compared to other types of biometrics, the proposed SUBBASe uses fingerprints for user authentication when joining a WSN. Moreover, a fingerprint authentication method does not require any additional hardware [25]. Users can easily provide biometric information on their own device such as a PDA or PC. To access information from the network, user can send message to sensor node directly that will be in the range of its query device. In order to query sensor node, user may use any device with fingerprint sensor, i.e., mobile phone, PDA, notebook, etc. Multiple users can be allowed to access wireless sensor network through their own mobile devices. Before network deployment, all sensor nodes are preloaded with secret information, i.e., x_0. Due to this secret information trusted node authenticates sensor node which will entertain request of user. SUBBASE considers a WSN of Mica2 sensor nodes and base station. Base station (TN) acts as authenticator of both the user and the sensor node. TN is trustworthy and secure with dominant resources in terms of memory, energy, and computation. Network architecture is shown in Figure 1. There are two main phases: an enrolment phase, followed by a user authentication phase. All symbols and notations used in this paper are described in Table 2.

3.1. How SUBBASe Algorithm Works

(1) Enrolment Phase

(i) In this phase, users register initially with a trusted node. The users then capture their biometric features and calculate a hash on them. They then submit their ID_u and hash value to the trusted node, as indicated in

$$m1 = [IDu, v] \quad \text{where } v = h(biou) \tag{1}$$

(ii) After a successful registration, trusted node computes s, as shown in (2) and sends it to the user. The value of x_o is network information applied by trusted node to extract their requested information.

$$m2 = [s] \quad \text{where } s = h(IDu \parallel xo) \tag{2}$$

Table 2: Symbols and notations.

Abbreviation	Description
ID_u	Identity of user
h(.)	One way hash function
$E_{wi}()$	Encryption of message
$D_{wi}()$	Decryption of message
‖	Concatenation operator
Δt	Time interval for transmission delay
x_o	Secret value known to TN
bio_u	Biometric of user
RI	Requested Information of user

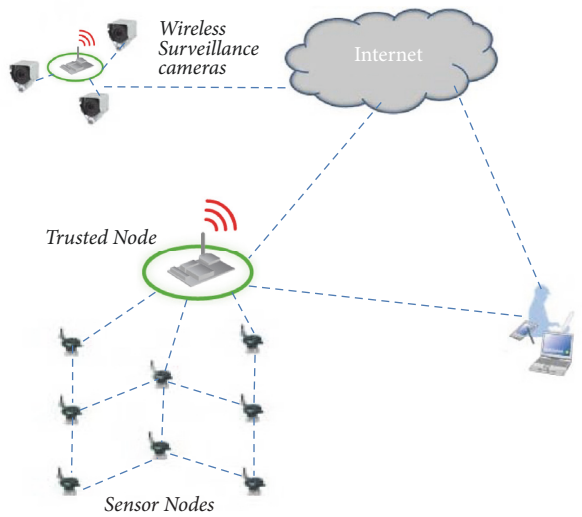

Figure 1: Depiction of wireless sensor network environment.

(2) Authentication Phase

(i) In this phase, users again capture their fresh biometric information and calculate a hash on it and then send this hash, ID_u and the requested information to the sensor node, as shown in (3). The fresh biometric information of a user is $v' = h(bio_u)$. In (3), RI is the requested information and T_0 is a user's current time stamp.

$$m3 = \left[IDu, v', RI, T0\right] \tag{3}$$

(ii) The sensor node receives a message at time T_1 and first checks the time stamp. If T_1-$T_0 \geq \Delta T$, the request is rejected; otherwise, this request is forwarded for user verification with its own *ID* to a trusted node at time T_2, as shown in (4).

Here, ΔT is the estimated time interval, and SN is the sensor node identification, which is responsible for handling user queries.

$$m4 = \left[IDu, y, T2\right] \quad \text{where } y = h\left(IDu \| v' \| SN\right) \tag{4}$$

(iii) After receiving the message at time T_3, the trusted node first checks the freshness of the message. If T_3-$T_2 \geq \Delta T$, then the request is rejected; otherwise, the trusted node checks y, as indicated in (5).

$$y = h\left(IDu \| v' \| SN\right) \tag{5}$$

(iv) The trusted node compares v and v'. If $v \neq v'$, then the trusted node sends a reject message to the sensor node.

$m_5 = [reject]$

The sensor node forwards the message to the user.

$m_6 = [reject]$

Otherwise, TN sends the message m_7 to SN.

$m_7 = [In\text{-}Progress]$

(v) When a message with a state label *In-Progress* is sent to the user, it indicates that the user can proceed to the authentication process. If a successful match occurs, the trusted node calculates *s*, as shown in (2), and

Start:
Step 1: $U \longrightarrow TN : [IDu, v]$
Step 2: $TN \longrightarrow U : [s]$
Step 3: $U \longrightarrow SN : [IDu, v', T0, RI]$
Step 4: $SN \longrightarrow TN : [IDu, y, T2]$
If
$v \neq v'$ then
exit
else
Step 5: $TN \longrightarrow SN : [in - progress]$
$TN \longrightarrow SN : [Accp, s, T4]$
Step 6: $SN \longrightarrow U[Accp, e, T6]$
Stop

Algorithm 1: Registration and authentication phase messages.

sends the message to the sensor node, as indicated in (6) at time T_4.

$$m8 = [Accp, s, T4] \tag{6}$$

(vi) The sensor node receives this message at T_5 and checks the timestamp. If T_5-$T_4 \geq \Delta T$, then the request is rejected; otherwise, *SN* computes *s*, as indicated in (2) and conducts data packing, as shown in (7) and (8).

$$d = (RI) \tag{7}$$

$$wi = h(IDu \| T6 \| s) \tag{8}$$

(vii) The sensor node uses w_i as a session key which is shared between the user and sensor node. Here, $E_{wi}(d)$ is the encryption of the requested information (RI) of the user, as indicated in (9).

$$m9 = [Accp, e, T6] \quad \text{where } e = [Ewi(d)] \tag{9}$$

(viii) The user checks the time. If T_7-$T_6 \geq \Delta T$, then the time is invalid; otherwise, it proceeds with a response. If the user is legal and holds *s*, the user will be able to access the network information. The user first computes w_i and then decrypts the message with function D_{wi}. In this way, the user obtains the requested information, as indicated in (10).

$$wi = [h(IDu \| T6 \| s)], Dwi(e) \tag{10}$$

The entire authentication algorithm of SUBBASe is summarized in Algorithm 1.

4. Security Analysis

This section demonstrates the strength of the proposed protocol from a network security perspective. We show that our proposed authentication technique has been designed to prevent various types of security attacks in WSNs, as discussed in the literature.

4.1. Stolen-Verifier Attack

If an attacker steals user information from a trusted and/or sensor node and attempts to cheat the involved entities:

this scheme can prevent a stolen-verifier attack because no password or verifier table is used. Therefore, an attacker cannot steal user information from a trusted and/or sensor node. Schemes that preserve such password tables to confirm a user login may suffer from this type of attack. This threat is solved with SUBBASe; however, because user biometrics is used for the network login.

4.2. Message Confidentiality

If an attacker overhears a message exchanged between a legal user and a sensor node and obtains secret network information:

with SUBBASe, message confidentiality is provided because user requested information is encrypted. If requested information is transmitted without encryption and passes through a public channel, the attacker can easily sniff the network information. Existing protocols do not provide message confidentiality. SUBBASe provides this service as encrypted requested information, $E_{sk}(d)$, is sent across a network.

4.3. Provide Mutual Authentication

If both parties are not authenticated during conversation:

SUBBASe provides mutual authentication because all entities authenticate each other. For example, when a user sends a message to *SN*, *SN* then verifies it by sending a request to *TN*. In addition, *TN* verifies *SN* based on its *ID*, and when *TN* sends a message to the user, it verifies it through hidden parameter x_0.

4.4. Complicated Equipment

If there is requirement of additional hardware for the authentication process:

various storage devices such as smart cards are used for identification purposes, providing better security. However, they require special and expensive hardware, which not everyone can afford. With SUBBASe, users can easily use any recognition interface without the need for an additional device using its Mobile or PDA. This is beneficial to both users and vendors and can increase the network efficiency and user convenience. Through the development of new technologies, mobile or laptop devices can easily be used to identify numerous types of biometrics.

4.5. Guessing Attack

If an attacker is able to guess the password or security parameters used for authentication purpose:

SUBBASe offers resistance to a guessing attack because users provide biometric features at the time of registration and at the time of authentication. Thus, an attacker cannot guess the user's biometrics. Preventing a guessing attack is crucial in systems that are based on password security.

4.6. Data Integrity

If an attacker obtains a message transmitted between a sensor node and a legal user and makes changes to the content:

this service provides assurance that communicated data cannot be changed by an unauthorized entity. With SUBBASe, data integrity is provided using a one-way hash function, i.e., $m_4 = [ID_u, y, T_2]$, where $y = h(ID_u \| v' \| SN)$, which is a message sent by the user to *TN*. Similarly, all communicated messages are sent in the same way, which cannot be modified by an attacker.

4.7. Prevent Replay Attack

If an attacker obtains previously communicated messages and starts communicating after acquiring the same rights as a legal user:

SUBBASe uses a time stamp to prevent this type of an attack. Suppose an attacker captures $m_3 = [ID_u, RI, v', T_0]$ and wants to replay the same message to *TN*. If the attacker perceives the communication message, the attacker cannot get verify because T_1-$T_0 \geq \Delta T$, where T_1 is the time stamp when the replayed message is received by *TN*. Time synchronization for wireless sensor networks is a very active research area [26–28] and it can easily be used for prevention of replay attack.

4.8. Prevent Node Compromise Attack

If an attacker succeeds in capturing a sensor node and collects all sensitive data from it:

if user is allowed to get data directly from sensor node without authenticating the node, it will result in the attack "node compromise". In SUBBASE sensor node is first authenticated by trusted node after authentication; sensor node is able to respond to the query of user that prevents node compromise attack. Also user hash of biometric is saved on the node which cannot be retrieved, as hash is a one-way function.

4.9. Network Traffic Attack

If an attacker succeeds in sending too much traffic on network like DDos attacks, with the intention to disrupt network functionality:

in SUBBASE protocol, authentication messages are reduced as task is divided among TN and SN to authenticate users. TN authenticates SN and user simultaneously, in order to avoid other malicious attacks like Denial of Service (DOS) attack. For example, if SN is not authenticated by TN, then any malicious node can send multiple fake authentication request messages/packets over the network that will results in increasing the network's traffic, depleting the resources of TN, and denying services to original users.

Table 3 provides an enhanced comparison of the different types of previous schemes against SUBBASe with respect to message confidentiality, network attacks, security parameters, and the requirement of any additional hardware devices for authentication.

5. Proof of SUBBASE Using BAN Logic

In this section we will use Burrows-Abadi-Needham (BAN) logic to validate that user and sensor node generate a valid and fresh session key for message exchange. Basic symbols used for BAN logic are described in Table 4.

The ban logic also provides the following basic rules:

(1) Message meaning rule:

$$\frac{U \mid\equiv U \overset{K}{\longleftrightarrow} S, U \lhd \{X\} K}{U \mid\equiv S \mid\sim X} \tag{11}$$

(2) Nonce verification rule:

$$\frac{U \mid\equiv \#(X), U \mid\equiv S \mid\sim X)}{U \mid\equiv S \mid\equiv X} \tag{12}$$

(3) The believe rule:

$$\frac{U \mid\equiv (X, Y)}{U \mid\equiv X} \tag{13}$$

Table 3: Comparison between SUBBASe and existing schemes.

Attacks	Debiao	Yoon	Althobaiti	Kaul	Dongwoo	SUBBASe
Session key Establishment	No	No	Yes	Yes	Yes	Yes
Message Confidentiality	No	No	Yes	Yes	Yes	Yes
Prevent Integrity	Yes	Yes	Yes	No	Yes	Yes
Prevent Replay Attack	Yes	Yes	Yes	Yes	Yes	Yes
Prevent Guessing Attack	Yes	Yes	Yes	No	Yes	Yes
Provide Mutual Authentication	Yes	Yes	Yes	Yes	Yes	Yes
Avoid Impersonation attack	No	No	No	No	Yes	Yes
Avoid Node Compromise Attack	No	No	Yes	No	Yes	Yes
Complicated Hardware Needed	Yes	Yes	No	Yes	Yes	No
Avoid Insider Attack	Yes	No	Yes	Yes	Yes	No

Table 4: Symbols for BAN Logic.

Symbol	Meaning
U $\mid\equiv$ X	U *Believe* the Statement X
#X	The Statement X is *Fresh*
U $\mid\sim$ X	U once *Said* X
$\{X\}_K$	Formula X is *encrypted* by key K
$\langle X\rangle_K$	Formula X is *combined* by key K
U $\Longrightarrow$ X	U *Control over* the Statement X
U $\triangleleft$ X	U *See* the Statement X
U $\overset{K}{\longleftrightarrow}$ S	U and S shared key K for communication
SK	Session Key
T	Time Stamp

(4) Freshness rule:

$$\frac{U \mid\equiv \#(X)}{U \mid\equiv \#(X,Y)} \tag{14}$$

(5) Jurisdiction rule:

$$\frac{U \mid\equiv S \mid\Longrightarrow X, U \mid\equiv S \mid\equiv X}{U \mid\equiv X} \tag{15}$$

We have the following goals to prove the validity of requested information and freshness of session key used for communication:

Goal 1. $U \mid\equiv \#(SK)$

Goal 2. $U \mid\equiv \#(RI)$

The message exchange of SUBBASE in idealized form is given below:

Message 1. $U \longrightarrow SN : \langle IDu, v', RI\rangle$

Message 2. $SN \longrightarrow TN : \langle IDu, Y\rangle$

Message 3. $TN \longrightarrow SN : (s)$

Message 4. $SN \longrightarrow U : T, \{RI\}sk$

To proceed with the proof, we have defined the following assumptions:

(i) A1: $U \mid\equiv SN \Longrightarrow SK$

(ii) A2: $SN \mid\equiv TN \overset{X_O}{\longleftrightarrow} SN$

(iii) A3: $TN \mid\equiv TN \overset{X_O}{\longleftrightarrow} SN$

(iv) A4: $SN \mid\equiv SN \overset{SK}{\longleftrightarrow} U$

(v) A5: $U \mid\equiv SN \mid\sim T$

(vi) A6: $U \mid\equiv TN \mid\sim s$

(vii) A7: $U \mid\equiv \#(RI)$

Detailed Process of Proof Is as Follows

Step 1. According to M4

$$V1 : SN \triangleleft T, \{RI\}\, SK \tag{16}$$

Table 5: Comparison of computational time between SUBBASe and existing schemes.

Protocols	Registration	Login+ Authentication	Total	Total time
Yoon	3 T_H	10 T_H	13 T_H	47.26 ms
Debiao	3 T_H	8 T_H +4t_{sym}	11 T_H +4t_{sys}=15 T_H	54.54 ms
Althobaiti	2 T_H	6 T_H + 2T_{MAC} +4 RC_5	8T_H + 2T_{MAC} +4 RC_5	36.37ms
Kaul	6T_H	16T_H	22T_H	79.97ms
Dongwoo	6T_H	14 T_H	20 T_H	72.7ms
SUBBASe	2T_H	7T_H +2Trc5	9 T_H +2*T*rc5	33.24 ms

Step 2. According to V1 and A4 and message meaning rule

$$V2 : U \mid\equiv SN \mid\sim RI \tag{17}$$

Step 3. According to A7 and V2 and nonce verification rule

$$V3 : U \mid\equiv SN \mid\equiv RI \tag{18}$$

Step 4. According to V3, A1 and believe rule

$$V4 : U \mid\equiv (RI, SK) \tag{19}$$

Step 5. According to A7 and V4 and freshness rule

$$\begin{aligned} V5 : U \mid\equiv \#(SK) \quad (GOAL\ 1) \\ V6 : U \mid\equiv \#(RI) \quad (GOAL\ 2) \end{aligned} \tag{20}$$

6. Performance Analysis

We use a mathematical model to examine the performance of SUBBASe and how it compares with existing schemes. The comparison is based on a computation of the time and energy consumption. We selected RC5 which is most suitable for implementation on resource constrained devices. The time to encrypt and decrypt a message using RC5 on a mica2 node is 0.26ms [29]. Similarly we chose SHA-1, whose performance time for a one-way hash function on mica2 is 3.636ms [30].

With Yoon et al.'s scheme 13 hash computation operations are required. A user needs one hash operation during the registration phase, and three during the authentication phase. A sensor node needs three hash calculations, and a trusted node needs two hash operations during the registration phase and four during the authentication phase. Similarly, the Debiao protocol [13] requires 11 hash computation operations and four T_{sym} operations for calculating a symmetric function (encryption/decryption) during the login and authentication phase. A user needs one hash function during the registration phase, and three hash operations and one T_{sym} operation for the encryption/decryption function during the authentication phase. A sensor node needs two hash calculations and one T_{sym} encryption/decryption function, and a trusted node requires two hash operations during the registration phase, and three hash operations and two T_{sym} operations during the authentication phase. A T_{sym} operation has the same computational cost as a hash operation, and thus the total number of hash operations with the Debiao protocol is 15. In the same manner, Althobaiti et al.'s scheme [15] requires two hash functions during the registration phase and six hash functions, i.e., two MAC functions and four RC5 functions, during the login and authentication phase. In Kaul et al.'s scheme user needs to perform 2 hash operations in registration phase while trusted node has to perform 4 hash operations. In login phase, user smart card performs 8 hash operations. During authentication, trusted node performs 6 and user performs 2 hash operations. Password change phase requires 10 hash operations by smart card. In Dongwoo et al.'s scheme user and trusted node both need to perform 3 hash operations in registration. In login phase, user side smart card performs 6 hash operations. During authentication, trusted node performs 5 and user performs 3 hash operations. Password change phase requires 7 hash operations by smart card.

With SUBBASe, one hash operation is required by a user during the enrolment phase; two hash operations and time for message decryption and three hash operations and time for message encryption are required by a sensor node; and three hash operations are required by a trusted node. Because a tiny sensor node has an inadequate amount of energy, the aim of our protocol is to reduce the computational cost of a sensor node. Although a user and a trusted node have sufficient resources to conduct multiple tasks, our scheme also minimizes the computational cost of a trusted node. Table 5 shows a complete picture of our comparison.

We used Matlab simulation to evaluate the strength and performance of the proposed security technique. Figure 2 shows a time computation graph of SUBBASe, and the Yoon et al., Debiao, Althobaiti et al., Kaul et al., and Dongwoo et al. schemes for multiple users accessing a network at the same time. When the number of users increases, the computational overhead for authentication also increases because more nodes are involved in the authentication process. With the SUBBASe scheme, when there is only one user, the computational overhead is 33.24ms, whereas with Yoon et al.'s scheme it is 47.26ms, in Debiao's method it is 54.54ms, with Althobaiti et al.'s approach it is 36.37ms, and with Kaul et al. and Dongwoo et al. it is 79.97ms and 72.7ms respectively. Results show that SUBBASe improves the network performance and its lifetime by reducing the amount of overhead.

Similarly, we calculated the energy consumption of SUBBASe and the other existing protocols. Main contributor for energy consumption in wireless sensor networks is data

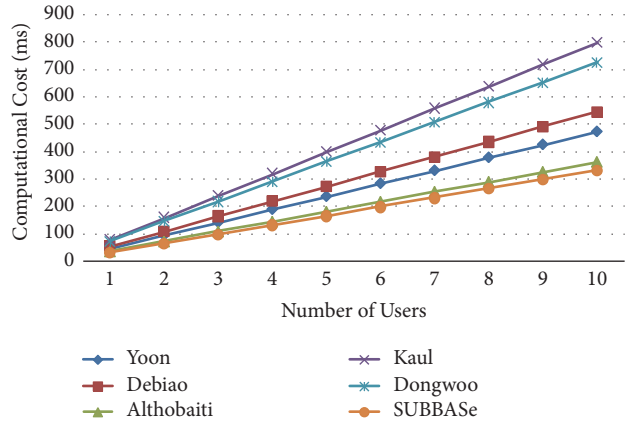

Figure 2: Computational overhead with respect to number of users.

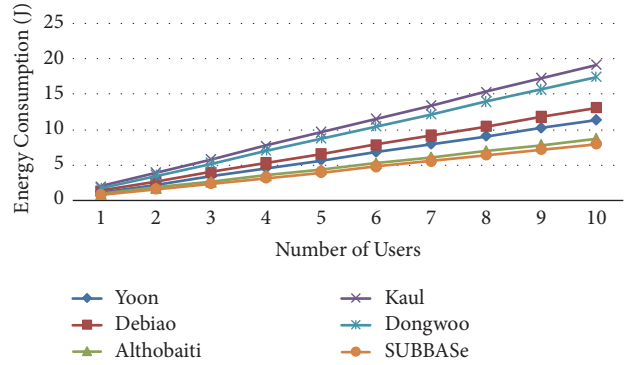

Figure 3: Energy consumption with respect to number of users.

transmission and reception, i.e., power consumed by antenna for sending and receiving messages. Just for comparison purpose, this paper focuses on calculating how much node power is consumed while performing the computations for authentication function.

To calculate the energy, we used "Computational Energy Cost" equation described in [31] and neglected the inactive state component. During the authentication process, sensor nodes do not go into inactive state. For mica2, node v = 3.0, and I = 8mA. In the equation, E denotes the consumption of energy, Q is the charge, I is the current, V is the voltage, and t is the time.

$$E = V \; x \; I \; x \; t \tag{21}$$

Figure 3 shows the energy consumption of SUBBASe, and the Yoon, Debiao, Althobaiti et al., Kaul et al., and Dongwoo et al. schemes with respect to the number of users. With SUBBASe, for one user, the energy consumption is 0.79J, whereas for Yoon et al.'s scheme it is 1.13J, for Debiao's approach it is 1.30J, for Althobaiti et al.'s method it is 0.87J, and for Kaul et al. and Dongwoo et al. schemes it is 1.9J and 1.7J respectively. Thus, the energy consumption of our proposed scheme is much less than that of the other existing security protocols. SUBBASe therefore proves to be more efficient, increasing the network performance and the lifetime by saving battery power of the nodes.

7. Conclusion and Future work

We proposed an authentication protocol that is based on the biometrics of users without the use of any traditional password or extra hardware devices. The proposed protocol simply proves the identity of the users through their biometrics. In addition, we designed our protocol to use simple and light computations. We mathematically analyzed the performance and security capability of SUBBASe and proved that it has better security features than other existing approaches. Moreover, based on a comparison with existing protocols, its computational cost and energy consumption are deemed to be suitable for resource constrained networks. In future BAN logic can be applied on SUBBASE to check its freshness property and its simulation can be done in security analysis tools.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by Basic Science Research through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A3B04031440). This study was also supported by 2017 Research Grant from Kangwon National University.

References

[1] C. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, 2003.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–105, 2002.

[3] Y. Faye, I. Niang, and T. Noel, "A survey of access control schemes in wireless sensor networks," *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 5, no. 11, 2011.

[4] H. Wang and Q. Li, "Achieving distributed user access control in sensor networks," *Ad Hoc Networks*, vol. 10, no. 3, pp. 272–283, 2012.

[5] P. Shantala, K. Vijaya, S. Sonali, and J. Rashique, "A survey on authentication techniques for wireless sensor networks," *Int. Journal of Applied Engineering Research*, vol. 7, no. 11, 2012.

[6] R. Rasmita and S. Itun, "A survey on authentication protocols for wireless sensor networks," *Int. Journal of Engineering Science and Technology*, vol. 3, no. 5, pp. 4253–4256, 2011.

[7] C. Jiang, C. B. Li, and H. Xu, "An efficient scheme for user authentication in wireless sensor networks," in *Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops/Symposia (AINAW '07)*, vol. 1, pp. 438–442, Ontario, Canada, May 2007.

[8] K. H. M. Wong, Z. Yuan, C. Jiannong, and W. Shengwei, "A Dynamic User Authentication Scheme for Wireless Sensor Networks," in *Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, vol. 1, pp. 244–251, IEEE, Taichung, Taiwan, June 2006.

[9] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[10] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'," *Sensors*, vol. 10, no. 3, pp. 2450–2459, 2010.

[11] J. Yuan, C. Jiang, and Z. Jiang, "A biometric-based user authentication for wireless sensor networks," *Wuhan University Journal of Natural Sciences*, vol. 15, no. 3, pp. 272–276, 2010.

[12] E.-J. Yoon and K.-Y. Yoo, "A new biometric-based user authentication scheme without using password for wireless sensor networks," in *Proceedings of the 2011 20th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE 2011*, pp. 279–284, France, June 2011.

[13] H. Debiao, "Robust biometric-based user authentication scheme for wireless sensor networks," *Cryptology ePrint Archive*, vol. 203, pp. 1–15, 2012.

[14] S. D. Kaul and A. K. Awasthi, "Security Enhancement of an Improved Remote User Authentication Scheme with Key Agreement," *Wireless Personal Communications*, pp. 1–17, 2016.

[15] S. Yu, J. Lee, K. Lee, K. Park, and Y. Park, "Secure Authentication Protocol for Wireless Sensor Networks in Vehicular Communications," *Sensors*, vol. 18, no. 10, 2018.

[16] O. Althobaiti, R. Mznah, and A. Abdullah, "An efficient biometric authentication protocol for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, 2013.

[17] D. Kang, J. Jung, H. Kim, Y. Lee, and D. Won, "Efficient and secure biometric-based user authenticated key agreement scheme with anonymity," *Security and Communication Networks*, vol. 2018, Article ID 9046064, 14 pages, 2018.

[18] R. Riaz, T.-S. Chung, S. S. Rizvi, and N. Yaqub, "BAS: the biphase authentication scheme for wireless sensor networks," *Security and Communication Networks*, vol. 2017, Article ID 7041381, 10 pages, 2017.

[19] M. Rakesh, *An improved user authentication protocol for hierarchical wireless sensor networks using elliptic curve cryptography [M. S. thesis]*, Department of Computer Science and Engineering, 2012.

[20] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *International Journal of Computer Science and Information Security*, vol. 4, no. 1, 2009.

[21] B. Debnath, R. Rahul, A. Farkhod, and C. Minkyu, "Biometric authentication: A review," *Science and Technology*, vol. 2, no. 3, 2009.

[22] W. Yang, J. Hu, S. Wang, and Q. Wu, "Biometrics based privacy-preserving authentication and mobile template protection," *Wireless Communications and Mobile Computing*, Article ID 7107295, 17 pages, 2018.

[23] Z. Han, L. Yang, S. Wang, S. Mu, and Q. Liu, "Efficient multifactor two-server authenticated scheme under mobile cloud computing," *Wireless Communications and Mobile Computing*, vol. 2018, 14 pages, 2018.

[24] E. Pagnin and A. Mitrokotsa, "Privacy-preserving biometric authentication: challenges and directions," *Security and Communication Networks*, vol. 2017, Article ID 7129505, 9 pages, 2017.

[25] B. Roli, S. Priti, and B. Punam, "Minutiae extraction from fingerprint images - a review," *International Journal of Computer Science Issues*, vol. 8, no. 5, 2011.

[26] D. Upadhyay, A. K. Dubey, and P. Santhi Thilagam, "Time synchronization problem of wireless sensor network using maximum probability theory," *International Journal of Systems Assurance Engineering and Management*, vol. 9, no. 2, pp. 517–524, 2018.

[27] L. Liu, G. Luo, K. Qin, and X. Zhang, "An on-demand global time synchronization based on data analysis for wireless sensor networks," *Procedia Computer Science*, vol. 129, pp. 503–510, 2018.

[28] N. Xiong, M. Fei, T. Yang, and Y. Tian, "Randomized and efficient time synchronization in dynamic wireless sensor networks: a gossip-consensus-based approach," *Complexity*, vol. 2018, 16 pages, 2018.

[29] X. Le, M. Khalid, R. Sankar, and S. Lee, "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare," *Journal of Networks*, vol. 6, no. 3, pp. 355–364, 2011.

[30] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in *Proceedings of the Second International Conference on Embedded Networked Sensor Systems (SenSys '04)*, pp. 162–175, 2004.

[31] M. A. Razzaque and S. Dobson, "Energy-efficient sensing in wireless sensor networks using compressed sensing," *Sensors*, vol. 14, no. 2, pp. 2822–2859, 2014.