EAI Endorsed Transactions
on Pervasive Health and Technology

Research Article EAI.EU

An efficient and secure mutual authentication protocol in wireless body area network

M. Kumar.[1,*] and S.Z. Hussain[2]

[1, 2] Department of Computer Science, Jamia Millia Islamia, India

Abstract

INTRODUCTION: Wireless Body Area Network (WBAN) is an emerging field which is gaining a lot of attention in healthcare sector. It facilitates remote monitoring by gathering health related data using wearable bio-sensors based on Internet of Things (IoT). This technological advancement would significantly improve the tracking of fitness, health care delivery, medical diagnostics, early disease prediction, and associated medical dealings of any individual. Several challenges persist in WBAN due to its openness and mobility.
OBJECTIVES: The medical data is extremely sensitive and personal in nature therefore it must be protected at any cost while being communicated between nodes. Highly resource constrained tiny sized bio-sensors restrict the usage of energy seeking traditional cryptographic techniques and hence require lightweight schemes to be evolved to authenticate the sensor nodes for secure communication.
METHODS: Proposed lightweight mutual authentication based key agreement scheme is dependent on XOR operations and irreversible cryptographic hash functions. Scheme generates a session key to validate a pair of legitimate sensor nodes. BAN logic is used for formal verification and automatic security verification tool Scyther is used for the analysis of security protocol.
RESULTS: Proposed scheme lived up to expectation when tested using BAN logic and Scyther tool. The scheme is successfully tested on 15 security parameters which are identified after a careful literature survey whereas other peer works have testified no better than 67% of the total number of security parameters. The result indicates that the proposed scheme is lightweight as the communication cost and storage requirement of the scheme have outperformed rest of the 7 schemes during performance analysis.
CONCLUSION: Hence the proposed scheme is lightweight and efficient which is robust against modern attacks and performs better in comparison of its peers.

Keywords: wireless body area network, mutual authentication, wearable bio-sensors, key agreement, formal verification, BAN logic; Scyther tool, XOR operations, cryptographic hash functions

Received on 07 March 2023, accepted on 28 May 2023, published on 13 July 2023

Copyright © 2023 Kumar *et al.*, licensed to EAI. This is an open access article distributed under the terms of the CC BY-NC-SA 4.0, which permits copying, redistributing, remixing, transformation, and building upon the material in any medium so long as the original work is properly cited.

doi: 10.4108/eetpht.9.3114

1. Introduction

The recent advancement in microelectronics and embedded computing has given birth to IoT based micro devices which has provided a platform to develop and deploy many real time applications in numerous fields such as continuous remote health monitoring, early detection of chronic diseases, elderly care, military operations, security, automobile, multimedia, home appliances, sports and fitness program [1][2][3]. It is plausible to wear the bio-sensors either on body or even implanted within the body [4]. Wearable sensors are larger in size consequently having a bigger battery, more computational resources and larger storage in comparison to implantable sensors. Wearable sensors are generally

[*] Corresponding author. Email: manoj.rke77@gmail.com

used to measure blood pressure, heart rate, glucose level, respiration, pulse oximeter SpO_2, temperature and pH level whereas implantable devices are used to measure brain liquid pressure, cardiac arrhythmia and endoscopy [5]. The invasive body sensors are small, thin, wireless enabled and operate at low power [6].

WBAN is an ultra-short range wireless network of various bio-sensors, actuators and medical devices which provide a real time monitoring of its user with the help of remotely placed advanced diagnostic and imaging devices [7]. The world has seen the recent outbreak of Covid-19 disease which has caused disruptions to essential health services and exposed the weakness of the existing healthcare system to handle the situation in cases when the personal visits to the doctors or hospitals are largely prohibited. In absence of trained medical staff, WBANs can be deployed temporarily in case of any disaster situation. Sufferers can be monitored remotely by specialized medical staff and lives could possibly be saved. It is understood by the healthcare sector that the services provided by the existing healthcare system need a critical revision and an alternate system like WBAN is essentially required which can substantially substitute the existing healthcare settings. Certain diseases don't require constant hospitalization; consequently Out Patient Department (OPD) services would be largely replaced by WBAN. Remote monitoring and treatment is possible when the person is not bound to bed. It will reduce the burden on hospital beds and the risk of contagion. IoT based healthcare market has reached $300 billion in 2022 [8].

Sensor devices are attached to the human body. Coordinator collects the medical data through wireless communication and communicates to a remote server using established internet facilities. Remote server acts as an Electronic Health Repository (EHR) for long term storage and analysis of medical data to facilitate the doctors and caregivers. Machine Learning (ML) methods are being used over clouds for advanced diagnostics [9]. Users of WBAN are always worried about the safeguard of their personal data in the absence of security and privacy. Security and privacy are the two most important challenges since the adoption of computing devices in the healthcare domain [10]. Ultra-sensitive medical data cannot be left at the mercy of adversaries. Lack of security and privacy will deter the implementation of WBAN on a large scale due to trust deficit among its users [11]. The lack of standardization, openness and mobility also attract the adversaries to exploit the WBAN system [12][13][14]. Traditional cryptographic methods cannot be applicable in IoT based WBAN as the environment is extremely resource constrained in terms of computation capacity, storage and battery power [15]. To restrict the energy depletion of sensor nodes, specifically designed lightweight cryptographic methods would be suitable for WBAN [16]. Mutual authentication schemes with pre-deployed keys are highly efficient and found to be lightweight for the WBAN environment due to which they are popular among researchers as they require less mathematical computation.

This paper proposes a lightweight key agreement scheme based on mutual authentication of sensor nodes in WBAN. The proposed scheme performs XOR operations and hash functions. The scheme generates a session key at pair of nodes by exchanging few security parameters to verify the legitimate sensor nodes. Formal security analysis of the proposed scheme using BAN logic is discussed. Automatic security verification tool Scyther is used to verify the security of the proposed protocol.

The scheme is robust against anonymity and session unlinkability, eavesdropping attack, replay attack, man in the middle attack, sensor node capture attack, forward and backward secrecy, jamming and de-synchronization, impersonation attack, intermediate node (IN) compromise attack, HN spoofing attack, message integrity, brute force attack, collision attack, scalability, online/offline secret shared key guessing or hub node stolen database attack.

The major contributions of the paper are as follows

- An enhanced key agreement scheme is proposed which provides authentication between the nodes in WBAN topology.
- The proposed protocol is based on simple XOR operations and hash functions. It requires very limited resources which makes it efficient. It takes 496 bits of storage on sensor node (SN) and 160+320n+16m bits of storage on hub node (HN) where n is the number of sensor nodes in two-tier WBAN and m is the number of intermediate nodes (IN). Each sensor node performs 4 XOR operations and 5 hash functions whereas the controller node executes 5 XOR operations and 7 hash functions.
- The security of the scheme is analysed using rigorous formal security analysis using BAN logic and a very popular Scyther tool is used to perform the automatic security analysis.
- The proposed authentication scheme has improved in terms of storage and communication cost as compared to other existing authentication protocol for WBANs.

This paper is organized as follows: Section II discusses the related work. In section III, WBAN test bed is introduced. Section IV introduces the proposed scheme. In Section V, the scheme is validated using BAN logic. Scyther tool is used to perform the formal analysis in section VI of the paper. Section VII discusses the security analysis of the proposed scheme. Performance Analysis is presented in section VIII. Section IX provides the conclusion of the paper.

2. Related work

A number of key agreement schemes have been introduced to authenticate the node in the WBAN. Asymmetric key cryptography based proposed schemes require high resource utilization which are not found suitable for energy constraint environments like WBAN [17]. Symmetric key cryptography based lightweight authentication methods are gaining popularity. The related work is discussed in Table 1.

Table 1. Related work

S.No.	Reference	Cryptographic technique/method used	Limitation/Weakness of the scheme
1	Wong et al. [18], 2006	XOR, hash functions	Replay attack; forgery attack; stolen verification attack found be Das[19], 2009
2	Das[19], 2009	Third party user authentication	Node capture attack; impersonation attack found by Khan et al.[20], 2010
3	Khan et al. [20], 2010	Hashed password	Impersonation attack; stolen smart card attack found by Vaidya et al.[21], 2010
4	Al-Rassan et al. [22], 2011	Physiological values to generate key pairs with randomness characteristics	Physiological value based key agreement schemes are expensive and require error correction mechanism in addition
5	Zhang et al. [23], 2012	Electrocardiogram signals (Physiological values) are used to compute a common key	Errors in sampling makes the physiological value based scheme inefficient and slow
6	He et al. [24], 2013	Sub-keyed hash function and hardware implemented AES algorithm	Increased overhead due to the presence of AES in the protocol
7	Ma et al. [25], 2014	Zero knowledge proof (ZKP) based protocol, implemented on TinyOS based sensor nodes for WBAN	Method is costly due to the usage of public key. It is not immune to the security attacks like anonymity & session unlinkability, eavesdropping attack, forward & backward secrecy attack etc.
8	Liu et al. [26], 2014	Anonymous preserving protocol for WBAN	Not immune from stolen verification attack found by Zhao[27], 2014
9	Zhao [27], 2014	Elliptic curve cryptosystem for anonymity	Method does not offer real anonymity; it is possible to track the users because their pseudo identities are constant. The attack are found by Wang et al.[28], 2015
10	Wang et al. [28], 2015	Bilinear pairing	Suffering from impersonation attack found by Wu et al. [29], 2016
11	Gope et al. [30], 2016	Realistic lightweight anonymous authentication protocol for securing real time data in WSN	Scheme is not suitable in securing the session key found by Jolfaei et al.[31], 2017
12	Li et al. [32]	Anonymous mutual authentication and key agreement scheme for WBAN; considering two hop architecture	• Scheme is found vulnerable to impersonation attack & spoofing attack on sensor node & hub node respectively; Offline identity guessing attack found by Chen et al. [33], 2018 • Scheme has key-escrow problem found by Koya et al. [34], 2018
13	Chen et al. [33], 2018	XOR and hash function	Scheme is vulnerable to first level node capture attack as same as Li et al. [32], 2017
14	Koya et al. [34], 2018	Scheme is based on physiological signals; resists sensor & hub node impersonation attack and key escrow problem of Li et al. scheme	Kompara et al. [35], 2018 found that the scheme does not protect the untraceability and method is highly computational as it requires efforts in synchronizing the sensors, collecting and transforming the physiological signals
15	Kompara et al. [35], 2018	XOR, hash functions	Security analysis does not cover the protection against IN compromise attack, HN spoofing attack & stolen database attack.
16	Gupta et al. [36], 2019	XOR, hash function (authenticated key exchange)	Security analysis does not cover the protection against replay attack, jamming & de-synchronization attack
17	Li et al. [37], 2017	XOR, hash function	Ostad-Sharif et al. [38], 2019 found the scheme vulnerable to wrong session key agreement attack and de-synchronization attack
18	Ostad-Sharif et al. [38], 2019	XOR, hash function	Cryptanalysis performed by Alzahrani et al. [39], 2020 found that the

			scheme does not withstand against session specific temporary information attack, HN's master secret compromise attack and key compromised information attack
19	Khadem et al. [40], 2021	XOR, hash functions, static parameters	Security analysis does not cover impersonation attack, stolen database attack, HN spoofing attack etc.

Table 1 concludes that despite having a few improved key agreement schemes for WBAN environment, most of the schemes bear security loopholes and vulnerable to different security attacks and suffer from scalability issues. The presented work not only concerns about the lightweight and secured communication among the nodes but also provides a scheme which is immune to 15 different key attacks found after a careful literature review. The security features of the scheme are analysed using BAN logic and also validated the security findings using Scyther tool.

3. WBAN test bed

IEEE 802.15 Task Group 6 proposed 802.15.6 standard for WBAN in 2012, which may adopt two-hop and three-tier architecture [41]. The proposed scheme also follows the same architecture. Figure 1 illustrates the basic architecture of WBAN based on IoT consisting of three types of nodes- Sensor node (SN), Intermediate node (IN) and Hub node (HN). SN is a physical sensor placed on or implanted inside the body. SNs may be several to dozen in numbers. IN provides an access point to the underlying network of sensor nodes. Access point is a hand held device or mobile phone. It has more storage, computing and communication capacity than SN. HN is a local server (i.e. personal computer) which is rich in security, computing and storage resources. The collection of SNs and IN is called Tier-I (Intra-WBAN) of the network model. Tier-2 (Inter-WBAN) consists of different INs and HN. Tier 3(Beyond-WBAN) represents the already established network and responsible for beyond BAN communication.

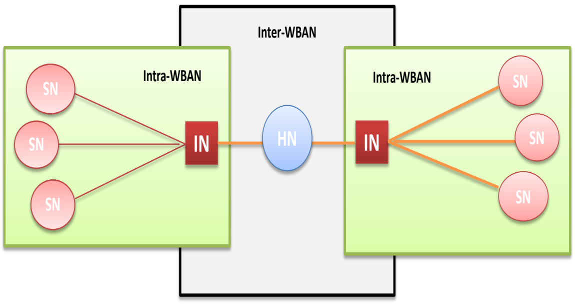


Figure 1. Two tier Wireless Body Area Network

The proposed protocol follows the Dolev-Yao threat model [42] [43]. It assumes that the communication takes place using an open (public) network and an adversary may gain the control of the network. It is possible for the attacker to intercept the communication, falsely inject the data, replay or alter the previously sent data. As the sensor node is not protected physically due to the cost constraint, these cannot be trusted in general. The attacker may capture the sensor nodes and extract the information from the storage of compromised sensor node.
The hub node is assumed to be trustworthy and it is not possible to compromise the node by an attacker.

4. Proposed scheme

Table 2. Parameters in the proposed scheme

S.No.	Symbol	Description
1	SA	System Administrator
2	SN	Sensor Node
3	IN	Intermediate Node
4	HN	Hub node or local server
5	ID_{SN}	Permanent Identification of Sensor Node
6	ID^*_{SN}	Id number of SN computed at HN
7	TID_{SN}	Temporary Identification of Sensor Node
8	TID^{++}_{SN}	Successive Temporary Identification of Sensor Node
9	ID_{IN}	Permanent Identification of Intermediate Node
10	K_{PS}	Session Key at SN
11	K^*_{PS}	Session Key at HN
12	K_{MS}	Master Secret Key of Hub Node
13	X_{SN}, Y_{SN}	Security parameters at SN
14	X^*_{SN}, Y^*_{SN}	Security parameters calculated at HN
15	r_{SN}	Nonce at SN
16	r^*_{SN}	Nonce computed at HN
17	T_1, T_2, T_3	Current time stamps
18	M_1, H_{SN}	Temporary security parameters at SN
19	H^*_{SN}	Security parameters calculated at HN
20	Z_{MS}, H_{MS}	Temporary security parameters at HN
21	H^*_{MS}	Security parameters calculated at SN
22	$\|\|$	Concatenation

23	$\oplus$	XOR
24	h( )	Hash function

A lightweight key agreement and mutual authentication protocol for WBAN is presented in this section. The symbols used in the scheme are shown in Table 2. The Sensor node (SN) mutually authenticates with the hub node (HN) and generates a session key K_{PS} . If WBAN is a star network, SN directly communicates with HN, otherwise in case of two hop networks SN communicates through IN. The proposed scheme has three phases-

Initialization Phase

Registration Phase

Authentication Phase

The initialization of the participants and registration of SNs and IN is realized by System Administrator (SA) in a secured environment. Authentication phase is responsible for mutual authentication of SN with HN. This phase is performed using a public network where fear of intrusion is always present.

Initialization Phase

SA generates a master secret key K_{MS} of HN and stores in HN memory.

Registration Phase

SA registers the SNs and IN as follows-

Step 1- For each SN, SA assigns a unique identity ID_{SN}.

Step 2- SA generates a temporary-id TID_{SN} of each SN.

Step 3- SA generates a unique identity ID_{IN} for intermediate node and stores in SN memory and HN memory.

Step 4- SA computes a security parameter $X_{SN} = h\ (K_{MS} \,||\, ID_{SN})$.

Step 5- SA computes another security parameter $Y_{SN} = K_{MS} \oplus ID_{SN} \oplus TID_{SN}$.

Step 6- SA stores the tuple (TID_{SN}, X_{SN}) into SN memory.
Step 7- For each SN, SA stores (TID_{SN}, Y_{SN}) into HN memory.

Authentication Phase

Step 1- SN generates a random nonce r_{SN}, captures the current time stamp T_1 and calculate the parameter $M_1=h(ID_{SN}) \oplus r_{SN}$..

Step 2- SN calculates another temporary security parameter $H_{SN} = h\ (X_{SN} \,||\, ID_{SN} \,||\, r_{SN})$.

Step 3- Message containing (TID_{SN}, H_{SN}, M_1, T_1) is sent to IN.

Step 4- IN attaches its own id ID_{IN} with the received message and relays the message (TID_{SN}, H_{SN}, M_1, T_1, ID_{IN}) to HN.

Step 5- HN checks the condition $|T2\text{-}T1| < \Delta T$ for the freshness of the message received from IN. T_2 is the current time stamp at HN and ΔT is the permissible time delay in the message. If the condition is not met, message is understood to be stale and discarded, otherwise the session is continued. The ID_{IN} value of message is matched with stored value of ID_{IN} in HN. If it is valid, following steps are performed-

- Search the HN database for TID_{SN} and retrieve the corresponding Y_{SN} from the table.
- Calculate $ID^*_{SN} = Y_{SN} \oplus K_{MS} \oplus TID_{SN}$
- Calculate $r^*_{SN} = M_1 \oplus h(ID^*_{SN})$
- Calculate $X^*_{SN} = h\ (K_{MS} \,||\, ID^*_{SN})$
- Calculate the session key $K^*_{PS} = h\ (X^*_{SN} \,||\, TID_{SN} \,||\, ID^*_{SN} \,||\, r^*_{SN} \,||\, T_1 \,||\, T_2)$
- Calculate $H^*_{SN} = h\ (X^*_{SN} \,||\, ID^*_{SN} \,||\, r^*_{SN})$
- Check if $H_{SN} \neq H^*_{SN}$ then terminate the session otherwise go to the next steps to continue.

Step 6- Generate a new temporary identity TID^{++}_{SN} and perform the following-

- $Z_{MS} = h\ (K^*_{PS}) \oplus TID^{++}_{SN}$
- $H_{MS} = h\ (K^*_{PS} \,||\, TID^{++}_{SN})$
- $Y^*_{SN} = (K_{MS} \oplus ID^*_{SN} \oplus TID^{++}_{SN}\ )$

Step 7- Replace the tuple (TID_{SN}, Y_{SN}) with (TID^{++}_{SN}, Y^*_{SN}) into HN memory for the next round.

Step 8- Send the reply message (Z_{MS}, H_{MS}, T_2, ID_{IN}) via an unsecured channel.

Step 9- IN removes its own id ID_{IN} with the received message and relays the message (Z_{MS}, H_{MS}, T_2) to SN.

Step 10- The SN checks the condition $|T_3\text{-}T_2| < \Delta T$ for the freshness of the message received from IN. T_3 is the current time stamp at SN and ΔT is the permissible time delay in the message. If the condition is not met, message is understood to be stale and discarded, otherwise the session is continued. If it is valid, following steps are performed-

Step 11- Calculate the session key $K_{PS} = h\ (X_{SN} \,||\, TID_{SN} \,||\, ID_{SN} \,||\, r_{SN} \,||\, T_1 \,||\, T_2)$

Step 12- Perform the following at SN-

- Calculate new $TID^{++}_{SN} = h\ (K_{PS}) \oplus Z_{MS}$
- Calculate $H^*_{MS} = h\ (K_{PS} \,||\, TID^{++}_{SN})$

Step 13- Check $H^*_{MS} = H_{MS}$, continue the session, otherwise terminate the session.

Step 14- Replace temporary-id TID_{SN} with new temporary id TID^{++}_{SN} in SN.

Step 15- K_{PS} and K^*_{PS} established.

5. Formal proof of the scheme using BAN logic

Widely accepted BAN logic [44] [45] is used for formal security analysis and confirmation of scheme's mutual authentication and key agreement between a SN and HN. Following basic notations are used for BAN logic. Let P & Q are principals as per BAN logic and X & Y constitute the formula

- $P |\equiv X$: Principal P believes the statement X.
- $P \,\Delta\, X$: P sees X; A message containing statement X is received by the principal P. P can also repeat the same X to other principals .
- $\#(X)$: Fresh X; the statement X is fresh. X has not been utilised at earlier occasion, prior to the current run.
- $P | \Rightarrow X$: P controls X; Principal P has jurisdiction over statement X and should be trusted on this matter.
- (X, Y): X or Y is one part of this formula of (X, Y).
- $(X)_Y$: X is combined or encrypted with key Y.
- $P | \sim X$: P said X; the principal P sent a message X at some time. It is not sure that X was sent recently or long time ago but P believes X.
- $P \overset{k}{\leftrightarrow} Q$: Principals P & Q know the secret X and possibly to the parties trusted by P & Q.
- $\frac{P}{Q}$: If P is true then Q is also true

Inference rules or postulates:

Following includes the general inference rule or postulates for BAN logic-

IR1 (Message Meaning Rule): P and Q are communicating under key K. Using this rule, the existence of a parameter is assured which is possessed by both the parties.

$$\frac{P|\equiv P\overset{k}{\leftrightarrow}Q, P\Delta(X)_y}{P|\equiv Q|\sim X}$$

Message meaning rule is used to enable HN to verify the transmitted parameters from SN and vice versa.

IR2 (Nonce Verification Rule): This rule assures that P & Q trust on fresh X which is probably a random number.

$$\frac{P|\equiv \#(X),\ P|\equiv Q|\sim X}{P|\equiv Q|\equiv X}$$

Nonce verification rule is used to enable HN to verify the random number received from SN and vice versa.

IR3 (Jurisdiction Rule): This rule assures that P believes that Q controls X i.e. P assures that the request is coming from Q and none other than Q or simply Q is legitimate.

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

Jurisdiction rule is used to enable HN to have full control on the terminated SN parameters and vice versa.

IR4 (Freshness Rule): This rule assures that if X is fresh then the other component Y in the formula is also fresh.

$$\frac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$$

Freshness rule is used to enable HN to check whether the SN request is valid through freshness rule and vice versa.

IR5 (Belief Rule or Decomposition Rule): This rule assures that if a formula is true then all of their components are true.

$$\frac{P|\equiv (X,Y)}{P|\equiv (X)}$$

Belief rule is used to enable HN trusts SN and all its transmitted parameters and vice versa.

Initial Assumptions:

Following is the list of assumption for BAN logic-

$$H1:\ HN\ |\equiv SN \xleftrightarrow{X_{SN}} HN$$

$$H2:\ HN|\equiv \#\ (TID_{SN})$$

$$H3:\ HN\ |\equiv SN\ |\Rightarrow SN \xleftrightarrow{X_{SN}} HN$$

$$H4:\ SN\ |\equiv SN \xleftrightarrow{ID_{SN}} HN$$

$$H5:\ SN\ |\equiv (r_{SN})$$

$$H6:\ SN\ |\equiv HN \Rightarrow (SN \xleftrightarrow{K_{PS}} HN)$$

Idealized Forms:

$$IDf1:\ SN \longrightarrow HN: (SN \xleftrightarrow{X_{SN}} HN, r_{SN}, TID_{SN})_{SN \xleftrightarrow{ID_{SN}} HN}$$

$$IDf2:\ HN \longrightarrow SN: (SN \xleftrightarrow{X_{SN}} HN, r_{SN}, SN \xleftrightarrow{K_{PS}} HN)_{SN \xleftrightarrow{ID_{SN}} HN}$$

Goals:

$$Goal\ 1:\ HN\ |\equiv SN \equiv (SN \xleftrightarrow{X_{SN}} HN)$$

$$Goal\ 2:\ HN\ |\equiv (SN \xleftrightarrow{X_{SN}} HN)$$

$$Goal\ 3:\ SN|\equiv HN \equiv (SN \xleftrightarrow{K_{PS}} HN)$$

$$Goal\ 4:\ SN|\equiv (SN \xleftrightarrow{K_{PS}} HN)$$

Formal Verification

Based on Idealized forms, initial assumptions and inference rules, formal verification is as follows-

Lemma 1: Message Meaning Rule: HN verifies the transmitted parameters from SN

From Idf1, H1 and IR1

$$\frac{HN|\equiv\left(SN\xleftrightarrow{ID_{SN}}HN\right),\ HN\,\Delta\left(SN\xleftrightarrow{X_{SN}}HN, r_{SN},TID_{SN}\right)_{SN\xleftrightarrow{ID_{SN}}HN}}{HN|\equiv SN|\sim\left(SN\xleftrightarrow{X_{SN}}HN, r_{SN},TID_{SN}\right)} \tag{1}$$

Lemma 2: Freshness Rule: SN request is verified through freshness rule
From H2 and IR4

$$\frac{HN|\equiv \sharp\,(TID_{SN})}{HN|\equiv \sharp\,(SN\xleftrightarrow{X_{SN}}HN, r_{SN}, TID_{SN}} \tag{2}$$

Lemma 3: Verification Rule: HN verifies the random number.
From (1), (2) and IR2

$$\frac{HN|\equiv\sharp\left(SN\xleftrightarrow{X_{SN}}HN, r_{SN},TID_{SN}\right),\ HN|\equiv SN|\sim\left(SN\xleftrightarrow{X_{SN}}HN, r_{SN},TID_{SN}\right)}{HN|\equiv SN|\equiv\left(SN\xleftrightarrow{X_{SN}}HN, r_{SN}, TID_{SN}\right)} \tag{3}$$

Lemma 4: Belief Rule: HN trusts SN and all its transmitted parameters
From (3) and IR5, Goal 1 is achieved as

$$\frac{HN|\equiv SN|\equiv (SN\xleftrightarrow{X_{SN}}HN, r_{SN}, TID_{SN})}{HN|\equiv SN|\equiv (SN\xleftrightarrow{X_{SN}}HN)} \tag{4}$$

(It is same as Goal 1)

Lemma 5: Jurisdiction Rule: Now HN has full control on transmitted SN parameters
From H3 and (4), Goal 2 is achieved as

$$\frac{HN|\equiv SN|\Rightarrow\left(SN\xleftrightarrow{X_{SN}}HN\right),\ HN|\equiv SN|\equiv (SN\xleftrightarrow{X_{SN}}HN)}{HN|\equiv (SN\xleftrightarrow{X_{SN}}HN)} \tag{5}$$

(It is same as Goal 2)

Lemma 6: Message Meaning Rule: SN verifies the transmitted parameters from HN
From Idf2, H4 and IRI

$$\frac{SN|\equiv\left(SN\xleftrightarrow{ID_{SN}}HN\right),\ SN\,\triangle\,(X_{SN},\ X^{*}_{SN}, r_{SN}, SN\xleftrightarrow{K_{PS}}HN)_{SN\xleftrightarrow{ID_{SN}}HN}}{SN|\equiv HN|\sim\left(X_{SN},\ X^{*}_{SN}, r_{SN}, SN\xleftrightarrow{K_{PS}}HN\right)} \tag{6}$$

Lemma 7: Freshness Rule: HN request is verified through freshness rule
From H5 and freshness rule IR4

$$\frac{SN|\equiv \sharp(r_{SN})}{SN|\equiv \sharp\left(X_{SN},\ X^{*}_{SN}, r_{SN}, SN\xleftrightarrow{K_{PS}}HN\right)} \tag{7}$$

Lemma 8: Verification Rule: SN verifies the random number.
From (6), (7) and IR2

$$\frac{SN|\equiv\sharp\left(X_{SN},\ X^{*}_{SN}, r_{SN}, SN\xleftrightarrow{K_{PS}}HN, SN\xleftrightarrow{ID_{SN}}HN\right),\ SN|\equiv HN|\sim (X_{SN},\ X^{*}_{SN}, r_{SN}, SN\xleftrightarrow{K_{PS}}H}{SN|\equiv HN|\equiv (X_{SN},\ X^{*}_{SN}, r_{SN}, SN\xleftrightarrow{K_{PS}}HN)} \tag{8}$$

Lemma 9: Belief Rule: SN trusts HN and all its transmitted parameters
From (8) and IR5, Goal 3 is achieved as

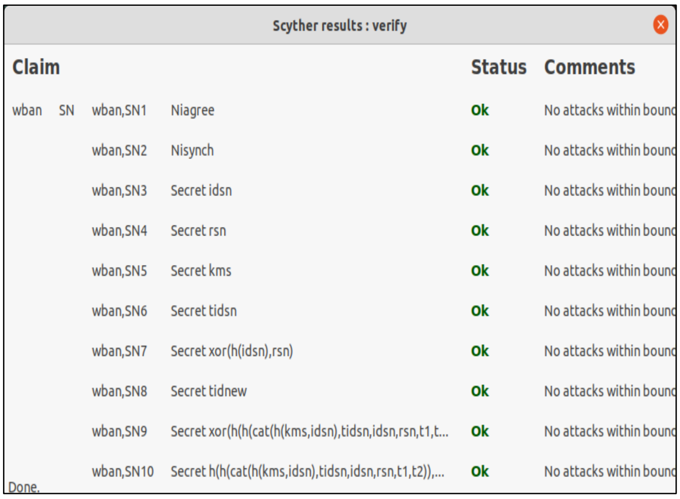
$$\frac{SN|\equiv HN|\equiv (X_{SN},\ X^{*}_{SN}, r_{SN}, SN\xleftrightarrow{K_{PS}}HN)}{SN|\equiv HN|\equiv (SN\xleftrightarrow{K_{PS}}HN)} \tag{9}$$

Lemma 10: Jurisdiction Rule: SN now obtains all the required parameters from HN and generates a session key at its end
From H6, (9) and IR3, Goal 4 is achieved as

$$\frac{SN|\equiv HN|\Rightarrow(SN\xleftrightarrow{K_{PS}}HN),\ SN|\equiv HN|\equiv (X_{SN},\ X^{*}_{SN}, r_{SN}, SN\xleftrightarrow{K_{PS}}HN)}{SN|\equiv (SN\xleftrightarrow{K_{PS}}HN)} \tag{10}$$

6. Analysis of the scheme using Scyther tool

Formal security validation of the proposed protocol is presented using a tool called Scyther [46], [47], [48]. Scyther tool is developed in Python and uses security protocol description language (SPDL). This tool follows Dolev-Yao threat model. Scyther tool analyses the security property of protocols, automatically validates the authentication and designed to detect data leakage. In case any attack is attack is detected, it is represented using graphical view [35]. This tool is applied to test the security claims which are defined by the tool itself. The security claims in the protocol are listed in the result window together with the findings of the verification. Result window contains single line for each of the claim. Figure 2-4 are the result windows of SN, IN and HN respectively. Result windows show that all the claims are true consequently determine that the protocol is true. If any protocol claim is found to be false, it will be displayed as attack in the result window.

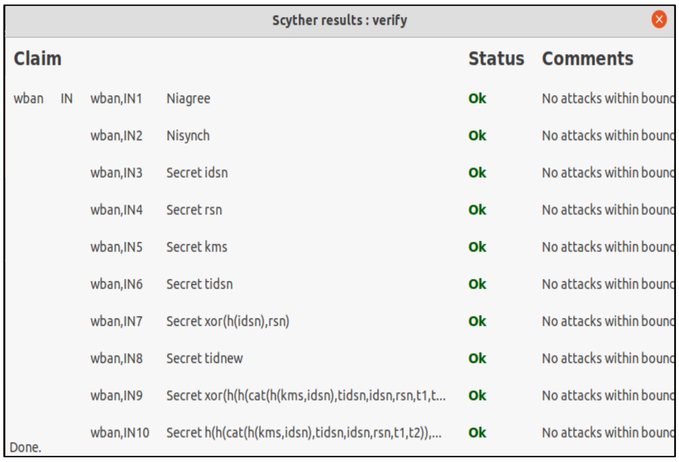


Scyther results : verify

Claim				Status	Comments
wban	SN	wban,SN1	Niagree	Ok	No attacks within bound
		wban,SN2	Nisynch	Ok	No attacks within bound
		wban,SN3	Secret idsn	Ok	No attacks within bound
		wban,SN4	Secret rsn	Ok	No attacks within bound
		wban,SN5	Secret kms	Ok	No attacks within bound
		wban,SN6	Secret tidsn	Ok	No attacks within bound
		wban,SN7	Secret xor(h(idsn),rsn)	Ok	No attacks within bound
		wban,SN8	Secret tidnew	Ok	No attacks within bound
		wban,SN9	Secret xor(h(h(cat(h(kms,idsn),tidsn,idsn,rsn,t1,t...	Ok	No attacks within bound
		wban,SN10	Secret h(h(cat(h(kms,idsn),tidsn,idsn,rsn,t1,t2)),...	Ok	No attacks within bound

Done.

Figure 2. Security claim verification at SN in Scyther

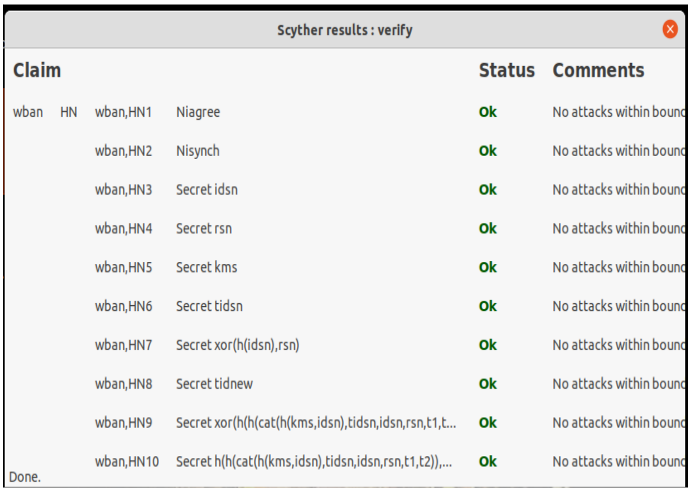


Scyther results : verify

Claim				Status	Comments
wban	IN	wban,IN1	Niagree	Ok	No attacks within bound
		wban,IN2	Nisynch	Ok	No attacks within bound
		wban,IN3	Secret idsn	Ok	No attacks within bound
		wban,IN4	Secret rsn	Ok	No attacks within bound
		wban,IN5	Secret kms	Ok	No attacks within bound
		wban,IN6	Secret tidsn	Ok	No attacks within bound
		wban,IN7	Secret xor(h(idsn),rsn)	Ok	No attacks within bound
		wban,IN8	Secret tidnew	Ok	No attacks within bound
		wban,IN9	Secret xor(h(h(cat(h(kms,idsn),tidsn,idsn,rsn,t1,t...	Ok	No attacks within bound
		wban,IN10	Secret h(h(cat(h(kms,idsn),tidsn,idsn,rsn,t1,t2)),...	Ok	No attacks within bound

Done.

Figure 3. Security claim verification at IN in Scyther



Scyther results : verify

Claim				Status	Comments
wban	HN	wban,HN1	Niagree	Ok	No attacks within bound
		wban,HN2	Nisynch	Ok	No attacks within bound
		wban,HN3	Secret idsn	Ok	No attacks within bound
		wban,HN4	Secret rsn	Ok	No attacks within bound
		wban,HN5	Secret kms	Ok	No attacks within bound
		wban,HN6	Secret tidsn	Ok	No attacks within bound
		wban,HN7	Secret xor(h(idsn),rsn)	Ok	No attacks within bound
		wban,HN8	Secret tidnew	Ok	No attacks within bound
		wban,HN9	Secret xor(h(h(cat(h(kms,idsn),tidsn,idsn,rsn,t1,t...	Ok	No attacks within bound
		wban,HN10	Secret h(h(cat(h(kms,idsn),tidsn,idsn,rsn,t1,t2)),...	Ok	No attacks within bound

Done.

Figure 4. Security claim verification at HN in Scyther

7. Security analysis

7.1. Anonymity and session unlinkability

The ID of Sensor Node (ID_{SN}) is not transferred wirelessly using public network rather a parameter M_1 is passed which contains a hashed value of ID_{SN} XORed with a random number r_{SN}. The property of hash function is that it is one way collision resistant i.e. ID_{SN} can never be retrieved from M_1. The other parameter H_{SN} also contains the hashed value of ID_{SN} which cannot be retrieved by the same hash property. The session key is calculated on the basis of a random number r_{SN} and temporary id TID_{SN} which are refreshed in each session. So, it is not possible for an adversary to link a current session with a previously completed session. Hence both the properties anonymity and session unlinkability are preserved in the proposed protocol.

7.2. Eavesdropping attack

The generation of session key K_{PS} depends upon X_{SN}, TID_{SN}, ID_{SN}, r_{SN}, T_1, T_2. Obtaining X_{SN}, ID_{SN}, r_{SN} from the transmitted message is not possible as these values are not being exchanged plain text rather the hash functions are involved in passing those values to other side of the network.

7.3. Replay attack

Every exchanged message is time stamped. If $|T2\text{-}T1| > \Delta T$, temporal inconsistency is detected and message would be rejected. The session key is also made dependent on time stamps. Any inconsistency would lead to generate mismatched session key. Fresh random value of r_{SN} cannot be revealed by transmitted value as it is exchanged using a check vector. TID_{SN} is also helpful in preventing replay attacks.

7.4. Man in the middle attack

Wireless transmission occurs in step 4/5 and 9/10 of authentication phase. In step 4, SN sends (TID_{SN}, H_{SN}, M_1, T_1) to IN whereas (TID_{SN}, H_{SN}, M_1, T_1, ID_{IN}) is used in step 5. Let us assume that the adversary intercepts the message exchanged in step 4 and tries to modify the message. As $H_{SN} = h\ (X_{SN} \parallel ID_{SN} \parallel r_{SN})$, parameters X_{SN}, ID_{SN} and r_{SN} are required to calculate the security parameter H_{SN}. H_{SN} follows the collision-resistant property of the one way hash function. It is also not possible for an adversary to compromise the value of X_{SN}, ID_{SN}, r_{SN} unless SN is captured physically. The session key K_{PS} depends upon the master secret key K_{MS} via X_{SN}. Compromising K_{MS} value is completely beyond the access of adversaries according to the Dolev-Yao threat model. In step 9, HN sends (Z_{MS}, H_{MS}, T_2, ID_{IN}) to IN whereas (Z_{MS}, H_{MS}, T_2) is used in step 10. Z_{MS} and H_{MS} parameters are based on hash functions. Z_{MS} and H_{MS} are based on K_{PS} which is not accessible to adversaries. As per birthday paradox, the size of input space would be the order of $O(2^{80})$with a matching probability of 0.5.

7.5. Sensor node capture attack

Suppose a Sensor Node (SN) is captured physically by an adversary. The effect of a captured node is analysed keeping in view of the security aspects of the other nodes of the network. A SN stores X_{SN} and TID_{SN} in its memory which can possibly get revealed. As $X_{SN} = h\ (K_{MS} \| ID_{SN})$, the value of the master secret key K_{MS} is secure as it is under the cover of collision resistant one way hash function. So, the value of K_{MS} is found to be secure even if a node is physically compromised consequently the rest of the network remains unaffected.

7.6. Forward and backward secrecy

Forward and backward secrecy ensures that even if the current session key is exposed, the previous and next session keys are not revealed. As session key $K^*_{PS} = h\ (X^*_{SN} \| TID_{SN} \| ID^*_{SN} \| r^*_{SN} \| T_1 \| T_2)$ is protected by collision resistant one way hash function, the master key, random variable, dynamic temporary parameters cannot be revealed from the same session.

7.7. Jamming and de-synchronization

An authentic protocol is vulnerable to a de-synchronization attack if the two involved parties are required to update their status at the same time. Suppose a jamming attack is attempted on a sensor node by an adversary, SN can attempt a reconnection to HN using the previously stored TID_{SN} and X_{SN}. HN also stores a unique $< TID_{SN}, Y_{SN} >$ tuple which represents ith node of the network.

7.8. Impersonation attack

In an impersonation attack an adversary can barge into a wireless body area network by an attempt to introduce a bogus SN. It would not be possible to invade an existing WBAN as the credentials $<TID_{SN}, Y_{SN}>$ of all the sensor nodes are pre-stored in HN. As $Y_{SN} = K_{MS} \oplus ID_{SN} \oplus TID_{SN}$, and if it is assumed for an adversary to guess ID_{SN} and TID_{SN}, the secret master key of HN (i.e. K_{MS}) cannot be assumed. Hence it is not possible to invade an existing WBAN using a forge SN.

7.9. Intermediate node (IN) compromise attack

If an adversary is able to get the physical access of Intermediate Node (IN), she will not be able to access any crucial security parameter with respect to the communication between SN and HN. IN is just an intermediary node which only contains a 16 bit ID_{IN} which is not going to reveal any information which can hamper the secure authentication process between SN and HN.

7.10. HN spoofing attack

The proposed scheme provides defence against Hub node spoofing attack because SN stores a security parameter $X_{SN} = h\ (K_{MS} \| ID_{SN})$ which depends upon a secret master key K_{MS} (a 160 bit long key). HN also contains another parameter $Y_{SN} = K_{MS} \oplus ID_{SN} \oplus TID_{SN}$ which is dependent on ID_{SN} and TID_{SN} of each of the SN involved. The value of K_{MS} and each of the SN's ID_{SN} and TID_{SN} cannot be guessed. Hence the protocol withstands against this attack.

7.11. Message integrity

The integrity of the message exchanged between SN to HN and vice-versa is preserved using collision resistant one way hash function. The parameters $H_{SN} = h\ (X_{SN} \| ID_{SN} \| r_{SN})$ and $M_1 = h(ID_{SN}) \oplus r_{SN}$ are exchanged from SN to HN and the parameters $Z_{MS} = h\ (K^*_{PS}) \oplus TID^{++}_{SN}$ and $H_{MS} = h\ (K^*_{PS} \| TID^{++}_{SN})$ are exchanged from HN to SN. All the parameters H_{SN}, M_1, Z_{MS} and H_{MS} use the hash function thus preserving the integrity of the message.

7.12. Brute force attack

In the proposed scheme, adversary has a weak chance to launch a successful brute force attack due to the length of the keys and other security parameters involved. Session key depends upon 6 parameters (X_{SN}, TID_{SN}, ID_{SN}, r_{SN}, T_1, T_2). Attacker has to brute force all the parameters to guess the correct session key. Hence it is not possible to launch a successful brute force attack in polynomial time on the proposed protocol.

7.13. Collision attack

The proposed protocol provides defence against collision attack in which attacker tries a number of combinations where two messages have the same value in hash function $h(M_1) = h(M_2)$. A good hash function always provides collision resistance. Hash functions are being used at overall 7 instances in our protocol. Hence the protocol is immune to collision attack.

7.14. Scalability

The protocol is designed to adjust the scalability issue in the network where the network can grow or shrink by adding or removing the nodes respectively without affecting the performance and security of the system. Nodes are first registered with HN. Some security parameters are also stored in SN. HN only allows the registered nodes to join the session and discards all illegitimate connection requests. A pre-validation reduces the overall communication between HN & SN and also to nullify the introduction of illegitimate sensors.

7.15. Online/Offline secret shared key guessing or hub node stolen database attack

The proposed scheme has a dynamic feature of refreshing the values used in generating the session key K_{PS}. The protocol contains randomized values such as TID_{SN}, TID^{++}_{SN} and r_{SN} which are updated in each round. Besides these, the current timestamp also takes part while generating the session key K_{PS}. The use of a one way cryptographic hash function at several steps strengthens the protocol. It is very hard for an attacker to guess the correct key by accessing the database as it is regularly updated.

7.16 Resisting against wrong session key agreement attack

A parameter $H_{SN} = h(X_{SN} \| ID_{SN} \| r_{SN})$ is evaluated at SN and transmitted to HN. At the end of HN, a corresponding parameter H^{*}_{SN} is calculated on the basis of $X^{*}_{SN,}$ ID^{*}_{SN}, r^{*}_{SN}. H_{SN} is compared with H^{*}_{SN} and then the session key is established. At the end of SN, H_{MS} is received from HN. H^{*}_{MS} is evaluated at SN. H_{MS} is compared with H^{*}_{MS} and then the session key is established. Hence the protocol is not only responsible for the generation of session key but also ensures the legitimacy of the session key at both the ends. The discussed mechanism provides resistance against wrong session key attack.

A comparison of the proposed protocol with other protocols on the above discussed parameters is provided in Table 3.

Table 3. Comparison of the proposed protocol with other protocols

Security Parameter	**Chen et al. [33]**	**Koya et al. [34]**	**Kompara et al. [35]**	**Ibrahim et al. [49]**	**Khan et al. [50]**	**Xu et al. [51]**	**Gupta et al. [52]**	**Ours**
SP1	Y	Y	Y	Y	Y	Y	Y	Y
SP2	N	Y	Y	Y	N	Y	N	Y
SP3	Y	Y	Y	Y	Y	Y	Y	Y
SP4	Y	Y	Y	Y	N	N	Y	Y
SP5	N	Y	Y	Y	N	Y	Y	Y
SP6	Y	Y	Y	Y	N	Y	Y	Y
SP7	N	Y	Y	N	Y	Y	N	Y
SP8	Y	Y	Y	N	N	Y	Y	Y
SP9	N	N	N	N	N	N	Y	Y
SP10	N	Y	N	Y	N	Y	N	Y
SP11	N	N	N	N	N	N	N	Y
SP12	N	N	N	N	N	N	N	Y
SP13	N	N	N	N	N	N	N	Y
SP14	N	N	N	N	N	N	N	Y
SP15	N	Y	Y	N	N	N	Y	Y
Total “Yes”	5	10	9	7	3	8	8	15

SP1: Anonymity and Session Unlinkability; **SP2:** Eavesdropping Attack; **SP3:** Replay Attack; **SP4:** Man in the Middle Attack; **SP5:** Sensor Node Capture Attack; **SP6:** Forward and Backward Secrecy; **SP7:**Jamming and De-Synchronization; **SP8:** Impersonation Attack; **SP9:** Intermediate Node (IN) Compromise Attack; **SP10:** HN Spoofing Attack; **SP11:** Message Integrity; **SP12:** Brute Force Attack; **SP13:** Collision Attack; **SP14:** Scalability; **SP15:** Online/Offline Secret Shared Key Guessing or Hub Node Stolen Database Attack

8. Performance analysis

In this section, storage space, communication cost, computational cost and energy consumption of SN and HN are discussed. The proposed scheme is also compared with other suggested schemes.

8.1. Storage requirement

According to Li et al.[40], the size of time stamps T_1, T2 and T_3 is $|T_1| = |T_2| = |T_3| = 32$ bits. The size of permanent –id of intermediate node ID_{IN} is 16 bits. It is also considered the same in this paper as well.

The size of the parameters $| ID_{SN} |$, $|TID_{SN} |$, $|K_{MS}|$ are assumed to be 160 bits long. SHA-1 is the hash function used in this scheme which affects the size of other parameters utilized in the scheme. The size of each of the parameters $|r_{SN}|$, $|X_{SN}|$, $|Y_{SN}|$, $|H_{SN}|$, $|M_1|$, $|K_{PS}|$ is 160 bits long. Each of the allied parameters $|ID^*_{SN}|$, $|X^*_{SN}|$, $|Y^*_{SN}|$, $|K^*_{PS}|$, $|r^*_{SN}|$, $|H^*_{SN}|$, $|H^*_{MS}|$ are also 160 bits long.

SN stores 4 parameters: ID_{SN}, TID_{SN}, X_{SN}, ID_{IN}. The size of storage $|ID_{SN}, TID_{SN}, X_{SN}, ID_{IN}|$ is 496 bits. HN stores 4 parameters: K_{MS} ,TID_{SN}, Y_{SN} , ID_{IN}. The size of storage $|(K_{MS}, TID_{SN}, Y_{SN}, ID_{IN})|$ is 160 + 320n + 16m where n is the number of SNs and m is the number of INs. A comparison of the storage cost of the proposed scheme with peer work is presented in Table 4.

Table 4. Comparison of Storage Cost with peer work

Peers	SN (in bits)	IN (in bits)	HN (in bits)
Chen et al. [33]	800	0	160n+160
Koya et al. [34]	640	640	320+160n
Kompara et al. [35]	640	16	640n +16m+160
Ibrahim et al. [49]	480	0	320n+320
Khan et al. [50]	640	0	160n+160
Xu et al. [51]	1280	32	768n+32m +512
Gupta et al. [52]	1056	288	288
Proposed	496	16	160+320n+16m

8.2. Communication cost

As discussed in authentication steps, SN relays 4 parameters (TID_{SN}, H_{SN}, M_1, T_1) to IN. The length of the message is 512 bits. IN attaches its own ID to the message before sending to HN. The message contains (TID_{SN}, H_{SN}, M_1, T_1, ID_{IN}) parameters. The length of the message is 528 bits. In turn, HN relays 4 parameters (Z_{MS}, H_{MS}, T_2, ID_{IN}) to IN. The length of the message is 368 bits. IN removes its own ID from the message and hence releases 3 parameters (Z_{MS}, H_{MS}, T_2) i.e. a total of 352 bits to SN. A comparison of the communication cost of the proposed scheme with peer work is presented in Table 5.

Table 5. Comparison of Communication Cost with peer work

Peers	SN->IN (in bits)	IN->HN (in bits)	HN->IN (in bits)	IN->SN (in bits)
Chen et. al [33]	672	672	640	640
Koya et al [34]	672	1344	960	480
Kompara et. al [35]	512	528	496	480
Ibrahim et. al [49]	480	640	640	480
Khan et. al [50]	832	832	800	800
Xu et. al [51]	832	864	1120	1088
Gupta [52]	1312	1344	1312	1320
Proposed	512	528	368	352

8.3. Computation & time cost

It is assumed that the computational time of XOR operation is t_{XOR} and 160-bits hash function is t_{hash}..t_{XOR} is extremely small as compared to t_{hash}. t_{XOR} can be assumed as zero ($t_{XOR} \approx 0$) without loss of any significant information. In the proposed scheme, 5 hash operations and 4 XOR operations are performed at SN. Computation time at SN is depicted as $5t_{hash} + 4t_{XOR} \approx 5t_{hash}$. There are 7 hash operations and 5 XOR operations performed at HN. Computation time at HN is depicted as $7t_{hash} + 5t_{XOR} \approx 7t_{hash}$.

Considering a 32-bit Cortex-M3 microcontroller at a frequency of 72 MHz with a memory of 512 KB, SHA-1 hash function takes 0.06ms [41] to execute once. Accordingly, SN will take 0.3ms to perform the overall computation. Using the same sensor, HN will take 0.42 ms to perform the computation at its end. A comparison of the computational cost of the proposed scheme with peer work is presented in Table 6.

Table 6. Comparison of Computational Cost and time with peer work

Peers	Node	Cost	Time
Chen et al. [33]	SN HN	$5t_{hash} + 5t_{XOR} \approx 5t_{hash}$ $8t_{hash} + 11t_{XOR} \approx 8t_{hash}$	0.3 ms 0.48 ms
Koya et al. [34]	SN HN	$3t_{hash} + 5t_{XOR} \approx 3t_{hash}$ $5t_{hash} + 10t_{XOR} \approx 5t_{hash}$	0.18 ms 0.3 ms
Kompara et al. [35]	SN HN	$3t_{hash} + 6t_{XOR} \approx 3t_{hash}$ $5t_{hash} + (n+7)t_{XOR} \approx 5t_{hash}$	0.18 ms 0.3 ms
Ibrahim et al. [49]	SN HN	$5t_{hash} + 2t_{XOR} \approx 5t_{hash}$ $8t_{hash} + 4t_{XOR} \approx 8t_{hash}$	0.3 ms 0.48 ms
Khan et al. [50]	SN HN	$5t_{hash} + 9t_{XOR} \approx 5t_{hash}$ $7t_{hash} + 14t_{XOR} \approx 7t_{hash}$	0.3 ms 0.42ms
Xu et al. [51]	SN HN	$5t_{hash} + 5t_{XOR} \approx 5t_{hash}$ $7t_{hash} + 9t_{XOR} \approx 7t_{hash}$	0.3 ms 0.42 ms
Gupta et al.[52]	SN HN	$7t_{hash} + 6t_{XOR} \approx 7t_{hash}$ $10t_{hash} + 11t_{XOR} \approx 10t_{hash}$	0.42 ms 0.60 ms
Proposed	SN HN	$5t_{hash} + 4t_{XOR} \approx 5t_{hash}$ $7t_{hash} + 5t_{XOR} \approx 7t_{hash}$	0.3 ms 0.42 ms

8.4. Energy consumption

At a room temperature of 27°C or 300°K, the microcontroller consumes 36 mA at 3.3V in active mode. Thus in active mode 118.8mW power is consumed. Energy consumption at SN and HN to perform the operations can be estimated. Sensor Node takes 0.3ms, so the energy consumption would be (118.8 x 0.3)/1000 = 0.03 mJ. Similarly, HN would consume (118.8 x 0.42)/1000 =0.04mJ. A comparison of the energy consumption of the proposed scheme with peer work is presented in Table 7.

Table 7. Comparison of Energy Consumption with peer work

Peers	SN (mJ)	HN (mJ)
Chen et al. [33]	.036	.057
Koya et al. [34]	.036	.048
Kompara et al. [35]	.021	.036
Ibrahim et al. [49]	.036	.057
Khan et al. [50]	.036	.05
Xu et al. [51]	.036	.049
Gupta et al.[52]	.042	0.6
Proposed	.036	.049

Conclusion

Several schemes were reviewed on fifteen key security parameters. It is found that none of the reviewed scheme follows all the parameters. Insecure key agreement protocols in WBAN environment can be proved fatal and may cost human life. In the proposed work, a lightweight mutual authentication protocol for one or two hop WBAN is presented. Efforts are made to keep a balance between security and performance as body sensor nodes are highly resource constrained. The protocol is verified using BAN logic as well as Scyther tool. Security parameters are refreshed in each round and accordingly the session key is generated. Comparison on the basis of 15 different security parameters, Storage cost, Communication cost, Computational cost and Energy consumption are also performed with other similar work in table 3 to 7 respectively. It is concluded that the proposed scheme has performed better than the other similar schemes.

References

[1] S. M. Riazul Islam, D. Kwak, M. H. Kabir, M. Hossain, A. Kyung- Sup Kwak, “The Internet of Things for Health Care: A Comprehensive Survey”, IEEE Access, Vol. 3, pp. 678-708, 2015.

[2] K. Wu, R. A. Laghari, M. Ali, A. A. Khan, “A Review and State of Art of Internet of things(IoT)”, Archives of Computational Methods in Engineering, Vol 29, no. 3, pp. 1395-1413, 2022.

[3] I. S. Huang, Y.H. Lu, M. Shafiq, A. A. Laghari, R. Yadav “A Generative Adversarial Network Model Based on Intelligent Data Analytics for Music Emotion Recognition under IoT”, Mobile Information Systems, Vol. 2021, Article ID 3561829, 8 pages, 2021.

[4] M. Kumar, "Security Issues and Privacy Concerns in the Implementation of Wireless Body Area Network", 2014 International Conference on Information Technology, Bhubaneswar, India, pp. 58-62, 2014.

[5] M. Kompara, M. Hölbl, “Survey on Security in Intra-body Area Network Communication”, Ad Hoc Networks, Vol. 70, pp. 23-43, 2018.

[6] R. Gravina and G. Fortino, "Wearable Body Sensor Networks: State-of-the-Art and Research Directions," IEEE Sensors Journal, Vol. 21, no. 11, pp. 12511-12522, 2021.

[7] K. A. Delgado-Vargas, G. Gallegos- Garcia, P. J. Escamilla-Ambrosio, “Cryptographic Protocol with Keyless Sensors Authentication for WBAN in Healthcare Applications”, Applied Sciences. Vol. 13, no. 3, p. 1675, 2023.

[8] S. Izza, M. Benssalah, K. Drouiche, “An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment”, Journal of Information Security and Applications, Vol. 58, p. 102705, 2021.

[9] M. Waqas, K. Kumar, A. A. Laghari, U. Saeed, M. M. Rind, A. A. Shaikh, F. Hussain, A. Rai, A. Q. Qazi “Botnet attack detection in Internet of Things devices over cloud environment via machine learning”, Concurrency and Computation Practice and Experience Vol. 34, no. 4, p. e6662, 2022.

[10] Nazir, Rashid, A.A. Laghari, K. Kumar, S. David, M. Ali. "Survey on Wireless Network Security." Archives of Computational Methods in Engineering Vol. 29, no. 3, pp. 1-20, 2022.

[11] S. Z. Hussain, M. Kumar, "Secured Key Agreement Schemes in Wireless Body Area Network-A Review", Indian Journal of Science and Technology Vol. 14 no. 24, pp 2005-2033, 2021.

[12] S. Mandal, “Provably secure certificateless protocol for wireless body area network”, Wireless Networks Vol. 29 no.3, pp. 1421-1438, 2023.

[13] A. A. Laghari, A. A. Khan, R. Alkanhel, H. Elmannai, S. Bourouis. "Lightweight-BIoV: Blockchain Distributed Ledger Technology (BDLT) for Internet of Vehicles (IoVs)", Electronics Vol. 12, no. 3, p. 677, 2023.

[14] A. A. Khan, A. A. Laghari, A. A. Shaikh, Z. A. Shaikh, A. K. Jumani, First Ed., CRC Press, 2022, 8, "Innovation in Multimedia Using IoT Systems", pp. 171-187.

[15] G. Mehmood, M. Z. Khan, A. Waheed, M. Zareei, E. M. Mohamed, ‘‘A trust-based energy-efficient and reliable communication scheme (trust-based ERCS) for remote patient monitoring in wireless body area networks,’’ IEEE Access, Vol. 8, pp. 131397–131413, 2020.

[16] Y. Yao, X. Chang, J. Misic, and V. B. Misic, ‘‘Lightweight batch AKA scheme for user-centric ultra-dense networks,’’ IEEE Trans. Cognit. Commun. Netw., Vol. 6, no. 2, pp. 597–606, 2020.

[17] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, “Authentication protocols for internet of things: A comprehensive survey”, Security and Communication Networks Vol. 2017, 2017.

[18] K. H. M. Wong, Y. Zheng, J. Cao, S. Wang, “A dynamic user authentication scheme for wireless sensor networks”, IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC’06), Vol. 1, p. 8, 2006.

[19] M. L. Das, “Two-factor user authentication in wireless sensor networks”, IEEE Trans. Wireless Commun. Vol. 8, no. 3, pp. 1086–1090, 2009.

[20] M. K. Khan, K. Alghathbar, “Cryptanalysis and security improvements of two factor user authentication in wireless

sensor networks", Sensors Vol. 10, no. 3 pp. 2450–2459, 2010.

[21] B. Vaidya, D. Makrakis, H.T. Mouftah "Improved two-factor user authentication in wireless sensor networks" 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications, pp. 600–606, 2010.

[22] I.A. Al. Rassan, N., "Secure & energy efficient key management scheme for WBAN-a hybrid approach", IJCSNS, Vol. 11, no. 6, p. 169, 2011.

[23] Z. Zhang, H. Wang, A.V. Vasilakos, H. Fang, "ECG-cryptography and authentication in body area networks", IEEE Trans Inf. Technol. Biomed. Vol. 16, no. 6, pp. 1070-1078, 2012.

[24] D. He, C. Chen, S. Chan, J. Bu, P. Zhang, "Secure and lightweight network admission and transmission protocol for body sensor networks", IEEE J. Biomed. Health Inform. Vol. 17, no. 3, pp. 664-674, 2013.

[25] L. Ma, Y. Ge, Y. Zhu, "Tinyzkp: A lightweight authentication scheme based on zero-knowledge proof for wireless body area networks", Wirel. Pers. Commun. Vol. 77, no. 2, pp. 1077-1090, 2014.

[26] J. Liu, Z. Zhang, X. Chen, K.S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks", IEEE Trans Parallel Distrib Syst. Vol. 25, no. 2, pp. 332-342, 2014.

[27] Z. Zhao, "An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem", J Med Syst. Vol. 38, no. 2, p. 13, 2014.

[28] C. Wang, Y. Zhang, "New authentication scheme for wireless body area networks using the bilinear pairing", J Med Syst. Vol. 39 , no. 11 , p. 136 , 2015.

[29] L. Wu, Y. Zhang, L. Li, J. Shen, "Efficient and anonymous authentication scheme for wireless body area networks", J. Med. Systems, Vol. 40 , no. 6 , p. 134 , 2014.

[30] P. Gope, T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks", IEEE Trans. Ind. Electron. Vol. 63 , no. 11 , pp. 7124–7132, 2016.

[31] A. Adavoudi-Jolfaei, M. Ashouri-Talouki, S.F. Aghili, "Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks", Peer-to-Peer Netw. Appl., Vol. 12, pp. 43-59, 2019.

[32] T. Li, Y. Zheng, T. Zhou,"Efficient anonymous authenticated key agreement scheme for wireless body area networks", Security and Communication Networks, Vol. 4167549, pp. 1-4167549, 2017.

[33] C. M. Chen, B. Xiang, T. Y. Wu, K. H. Wang, "An anonymous mutual authenticated key agreement scheme for wearable sensors in wireless body area networks", Appl. Sci. Vol. 8, no. 7, p. 1074, 2018.

[34] A.M. Koya, P. P. Deepthi, "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network", Comput. Netw. Vol. 140 pp. 138-151, 2018.

[35] M. Kompara, S. K. H. Islam, M. Holbl, "A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs", Computer Networks, Vol. 148, pp. 196-213, 2019.

[36] A. Gupta, M. Tripathi, T.J. Shaikh, A. Sharma, "A lightweight anonymous user authentication and key establishment scheme for wearable devices", Comput. Netw., Vol. 149, pp. 29-42, 2019.

[37] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.K.R. Choo, ‘‘Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks,’’ Comput. Netw., Vol. 129, pp. 429–443, 2017.

[38] A. O. Sharif, M. Nikooghadam, D. Abbassinezhad-Mood, "Design of a lightweight and anonymous authenticated key agreement protocol for wireless body area networks, " Int. J. Commun. Syst., Vol. 32 , no. 12, p. e3974, 2019.

[39] B. A. Alzahrani, A. Irshad, A. Albeshri, K. Alsubhi, and M. Shafiq, ‘‘An improved lightweight authentication protocol for wireless body area networks’’ IEEE Access, Vol.8, pp. 190855–190872, 2020.

[40] B. Khadem, A. M. Suteh, M. Ahmad, A. Alkhayyat, M. S. Farash and H. S. Khalifa, "An Improved WBSN Key-Agreement Protocol Based on Static Parameters and Hash Functions," IEEE Access, Vol. 9, pp. 78463-78473, 2021.

[41] M. S. Akbar, Z. Hussain, M. Sheng, R. Shankaran, "Wireless Body Area Sensor Networks: Survey of MAC and Routing Protocols for Patient Monitoring under IEEE 802.15.4 and IEEE 802.15.6", Vol. 22, no. 21, p. 8279, 2022.

[42] D. Dolev, A. Yao, "On the security of public key protocols," IEEE Trans. Inf. Theory Vol. 29, no. 2, pp. 198-208, 1983.

[43] T. Feng, S.M. Zhao, X. Gong "Formal Security Evaluation and Improvement of BACnet/IP Protocol Based on HCPN Model", International Journal of Network Security, Vol. 24, no. 2, pp. 193-205, 2022.

[44] M. Burrows, M. Abadi, and R. Needham, ‘‘A logic of authentication,’’ ACM Trans. Comput. Syst., Vol. 8, no. 1, pp. 18–36, 1990.

[45] A. M. Almuhaideb, H. A. Alghamdi, "Secure and Efficient WBAN Authentication Protocols for Intra-BAN Tier" Journal of Sensor and Actuator Networks Vol. 11, no. 3, p. 44, 2022.

[46] M. Tanveer, A. H. Zahid, M. Ahmad, A. Baz, H. Alhakami, ‘‘LAKEIoD: Lightweight authenticated key exchange protocol for the Internet of drone environment,’’ IEEE Access, Vol. 8, pp. 155645–155659, 2020.

[47] C. J. F. Cremers, Scyther: Semantics and Verification of Security Protocols. Eindhoven, The Netherlands: Eindhoven Univ. Technology, 2006.

[48] L. Viganò, ‘‘Automated security protocol analysis with the AVISPA tool,’’ Electron. Notes Theor. Comput. Sci., Vol. 155, pp. 61–86, 2006.

[49] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid, and V. Odelu, ‘‘Secure anonymous mutual authentication for star two-tier wireless body area networks,’’ Comput. Methods Programs Biomed., Vol. 135, pp. 37–50, 2016.

[50] H. Khan, B. Dowling, and K. M. Martin, ‘‘Highly efficient privacy-preserving key agreement for wireless body area networks’’ 2018 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun. /12th IEEE Int. Conf. Big Data Sci. Eng. (Trust Com / Big Data SE), pp. 1064–1069, 2018.

[51] Z. Xu, C. Xu, W. Liang, J. Xu, and H. Chen, ‘‘A lightweight mutual authentication and key agreement scheme for medical Internet of Things,’’ IEEE Access, Vol.7, pp. 53922–53931, 2019.

[52] A. Gupta, M. Tripathi, and A. Sharma, ‘‘A provably secure and efficient anonymous mutual authentication and key agreement protocol for wearable devices in WBAN,’’ Comput. Commun., vol. 160, pp. 311–325, 2020.