IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 5, 2020, accepted September 15, 2020, date of publication September 21, 2020,
date of current version October 8, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3025733

A Lightweight and Secure Anonymity Preserving Protocol for WBAN

ABDULLAH M. ALMUHAIDEB AND KAWTHER S. ALQUDAIHI
Department of Computer Science, College of Computer Science & Information Technology, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia

Corresponding author: Abdullah M. Almuhaideb (amalmuhaideb@iau.edu.sa)

This work was supported in part by the Imam Abdulrahman Bin Faisal University/College of Computer Science & Information Technology through the Deputyship for Research & Innovation, Ministry of Education, Saudi Arabia under Project Covid19-2020-067-CSIT.

ABSTRACT In the medical fields, wearable body area sensors network (WBAN) is playing a major role in maintaining user health by providing convenience service for the patient and doctors. However, sensor data transmission in an insecure communication channel enables the attacker from tampering the sensor data, disguising as a legitimate user, or intercepting the forwarded packets from its unprotected sources. A wide variety of secure authentication schemes were proposed to improve the communicated channels' reliability in protecting the user data. Moreover, those schemes are lacking the guarding of nodes anonymity, key management, and size. Thence, we propose a lightweight WBAN authentication with two protocols P-I for authentication and P-II for re-authentication to protect the nodes anonymity and increase the efficiency. Furthermore, our scheme employed better key management with high randomness of the security parameters to provide higher protection as a trade-off between security and efficiency. The scheme formal proof for the key agreement and mutual authentication is conducted through (Burrows Abadi Nadeem) BAN logic.

INDEX TERMS WBAN, anonymity, re-authentication, key management, key deletion, BAN logic.

I. INTRODUCTION

Internet of Things (IoT) is a platform of connected devices that communicate, share information with each other's and occupy a very wide concept with an increasing number of applications. One of the vital IoT applications that plays a major role in health monitoring is a wearable health monitoring system (WHMS) [1]–[4]. It enables doctors and patients to benefit from WHMS environment services. WBAN falls under the umbrella of the wider concept WHMS [5]–[7]. It assists the physicians in diagnosing allot of diseases either by attaching it in the patients' body or clothes for different readings [8]–[11]. WBAN consists of cheap and constrained memory sensors with limited processing capabilities, which makes it vulnerable against many attacks [12], [13]. Therefore, many schemes were proposed to maintain a trade-off between security and performance for WBAN. We need to understand the WBAN systems architecture to know exactly how the system components communicate among themselves. It consists of three major components, namely: hub node, foreign network node, and sensor node. First, the hub node works like a server that carries out the data collected from the sensor and delivers them to system administration for processing. Hub is the strongest entity of the communicating parties due to its high processing abilities and memory capacity. Second, the first-level node or foreign network (e.g. smartphone) holds less processing power than the hub node [14]. Third, the sensor node with the lowest processing power and memory, as depicted in fig1. After listing the

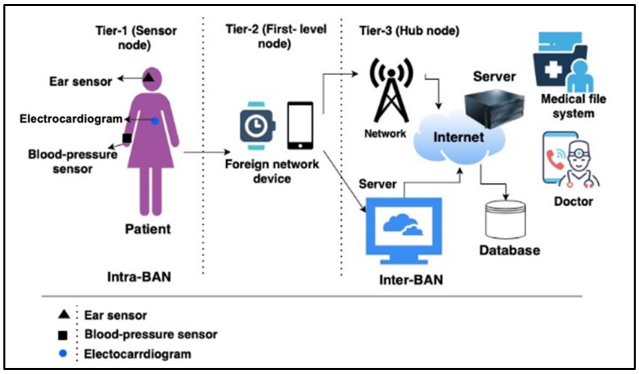

FIGURE 1. WBAN three-tier architecture.

The associate editor coordinating the review of this manuscript and approving it for publication was Mahdi Zareei.

communicated components, it clarifies what communication channels need to be protected in the WBAN platform. Consequently, the WBAN platform needs to concern the fulfilling of authentication between the authorize communicated parties, anonymity, un-traceability, integrity, and privacy [15]. Besides, there are two classifications of authentication models: distributed authentication model, where the hub node is not necessary for the authentication, and it can be offline. The second model is the centralized authentication in which the authentication occurs online, and the hub node is engaged in the verification [16].

In this paper, we focused on a centralized authentication model with three communicating entities: hub, first-level node, and second-level node. The main purpose is to increase efficiency and levitate the security by adding various random values in the proposed scheme. Through little high communication complexity, the scheme can attain a better trade-off between security and performance.

A. CONTRIBUTION AND MOTIVATION

In this paper, we enhanced Li *et al.* [17] scheme that uses a random nonce and complex interconnected parameter system with the least number of hash function. Although [17] has an efficient performance, it lacks perfect forward secrecy, un-traceability, node impersonation protection, key escrow protection, and session key protection according to [4], [9], [18]. Our motivation was to find the best contribution to Li *et al.* [17] scheme and improve it for better security and efficiency. After a comprehensive review of the related state of the art, we identified different flaws in Kompara *et al.* [9] scheme, which are foreign network node-sensor node replay attack, key management issue, hub impersonation attack, and anonymity problem. Our main contributions are as follows:

- Increase the efficiency of Kompara *et al.* [9] scheme by applying the re-authentication concept to decrease the sensor/hub communication and computation overhead.
- Produce an informal analysis and formal scheme proof by using BAN logic to prove the mutual authentication and key agreement along with informal security analysis. The analysis proved the scheme robustness against offline/online shared secret key guessing, brute force attack, replay attack, sensor/hub impersonation attack, session hijacking, and collision attack. Also, it offered some security and functionality features such as scalability, anonymity, un-traceability, integrity, and secure key deletion.
- We conducted a performance analysis in comparison with well-known schemes that show advantages in our scheme in a matter of computation and communication cost.

The rest of the paper is organized as follows. Section II contained the related work. Section III discussed and explained the new scheme. Section IV demonstrated a formal scheme proof by using BAN logic and informal security analysis. Section V discussed performance analysis. Finally, the conclusion and future work are interpreted in Section VI.

II. RELATED WORK

WBAN platform deals with sensitive substantial patient information that is essential to be protected against attacks. Since the patient information roams through non-secure channels, many schemes were created to strengthen user authentication [19]. Several schemes focus on the improvement of anonymity, privacy, forward secrecy, etc. without paying attention to design a model with strong key protection. Liu *et al.* [15] had proposed a scheme based on a dynamic password generation algorithm along with user biometric and smart cards for authentication. The scheme had achieved several security aspects like node anonymity, replay attack protection, and integrity, but according to [19] it did not consider the protection of the user biometric through using received signal strength indicator (RSSI) between nodes that makes [15] vulnerable to impersonation attack. Also, Arfaoui *et al.* [19] suggested two authentication protocols with edge sensor nodes and primary correlated nodes to collect the human body readings and send them to the controller node for authentication. Their scheme achieved anonymity for the nodes through using a one-way hash function, random nonce, and transaction sequence number to resist replay attack. Shen *et al.* [20] had proposed a scheme to enable the user from communicating anonymously in the cloud environment by utilizing asymmetric cryptography and message authentication code for integrity. The problem in [20] is its high computation time along with its weak protection to the secret random value, since its encrypted by employing the current time as a key. Another scheme proposed by Deng *et al.* [21] had employed bilinear pairing and data aggregation that can be recovered by the cloud center.

Furthermore, Alzahrani *et al.* [5] had cryptanalysis Lu *et al.* scheme [22] and showed that it is vulnerable to traceability, and has scalability issues. Alzahrani *et al.* [5] had utilized the elliptic curve based on the elliptic curve discrete logarithm and elliptic curve Diffie Hellman (ECCDH) to protect the user anonymity in a foreign network and remote area to enjoy home network services. Although that [5] had accomplished anonymity, un-traceability, and protection against privileged insider attack, the scheme is vulnerable to the DOS attack due to heavy calculations and parameters from the first level node that makes the attacker send bogus parameters values during the communication. Also, Odelu *et al.* [23] had proposed a lightweight authentication protocol for WBAN based on bilinear pairing to overcome privacy problems and the management of large numbers of public keys. Their scheme has two communicating entities client with sensor and network manager, which makes it secure against DOS attack, but it has high computation time and complexity.

All of the above-mentioned schemes had higher computation complexity than [17]. So, Xu *et al.* [4] had improved [17] by employing the complexity of ECC through exoring point on the curve with the master secret key in the initialization phase. Moreover, ECC is public-key cryptography with a key size 256bit to avoid brute force attacks. Although their scheme is protected against eavesdropping, sensor node capturing, sensor impersonation but it has lower efficiency in comparison to [17] and anonymity problem for access point id. Das *et al.* [24] had proposed a biometric authentication scheme between mobile and wearable devices, it is secure but has performance deficiency.

Likewise, Koya and P. P [18] had improved Li *et al.* [17] scheme by adding biometric authentication in foreign network node [18]. Their scheme is robust against key escrow problems and sensor node impersonation attacks, but it is vulnerable to foreign network node-sensor node replay attack, spoofing attack, the un-traceability problem according to [9], and anonymity problem. Batch authentication schemes were proposed in [24] to reduce the communication overhead in WBAN and 5G networks. Besides, Gupta *et al.* [25] had proposed a scheme to enhance the security of [18] but it has a scalability issue due to higher computation along with communication overhead problems. Also, Kompara *et al.* [9] suggested a lightweight scheme to overcome the sensor impersonation attack, guessing session key and the un-traceability in [17] by enabling the system to store the latest two session keys and keep track on the used keys.

Among all of the above schemes, Kompara *et al.* scheme [9] seems to be the best of all with minimum computation cost and communication overhead, as both [26], [27] are vulnerable to foreign network node-sensor replay attack, key management issue, hub impersonation attack, and anonymity problem. Also, Konan and Wang [28] stated that [9] had increased storage space problems. As a result, we discovered that re-authenticating a legitimate user in a short time along with deleting stored session keys has not been covered. So, we proposed new two protocols which are authentication protocol and re-authentication protocol to levitate the security and efficiency of [9].

III. PROPOSED PROTOCOL

In this section, we demonstrated our new authentication and key agreement protocol based on Kompara *et al.* scheme [9]. The scheme adopted [9] concept with improved security and efficiency by considering a higher anonymity level and un-traceability for each node. Also, we illustrated the symbols that had been used in the improved new scheme depicted in Table 1. Moreover, it represented the four phases of the scheme: initialization and registration, authentication, re-authentication, secure key deletion, and scheme comparison to [9].

TABLE 1. Symbols used in our protocol.

SYMBOL	DESCRIPTION
$\boldsymbol{SM}$	System manager
$\boldsymbol{SN}$	Sensor node
$\boldsymbol{FN}$	First level node
$\boldsymbol{HN}$	Hub node
$\boldsymbol{ID_{SN}}$, $\boldsymbol{ID_{SN}^{+}}$, $\boldsymbol{ID_{SN}^{++}}$	Sensor identity generated by SM/ updated ID_{SN} continuously.
$\boldsymbol{ID_{FN}, ID_{FN}^{+}}$	First level node identity generated by SM /hidden ID_{FN} updated
$\boldsymbol{ID'_{FN}}$, $\boldsymbol{ID_{FN}^{++}}$	FN node identity in each session
$\boldsymbol{ID_{STi}}$	Temporary identity chosen by the sensor with random generated number nonce
$\boldsymbol{ID_{HN}}$	Hub node identity generated by the system manager
$\boldsymbol{t1, t2, t3}$	Current time of the sensor and hub node
$\boldsymbol{seq, seq^{+}}$	Session Sequence number uniquely saved by the SM in DB of both HN and SN
$\boldsymbol{K_{MS}}$	Master pre-shared key generated by the system manager to both SN and HN
$\boldsymbol{SK}$	Session key computed by SM
$\boldsymbol{SK', SK^{*}}$ $\boldsymbol{PSK_{n}}$	Updated session key, new pre-shared key
$\boldsymbol{rand, rand^{*}, q}$ $\boldsymbol{, rand(i)}$	Generated random nonce/ updated random nonce
$\boldsymbol{DB_{HN}}$	Database of the hub node
$\boldsymbol{X1, A, B, V1}$	Authentication parameters
$\oplus$	Bitwise operator
$\boldsymbol{H}(.)$	One-way hash function
$\Vert$	Concatenation operation

A. INITIALIZATION AND REGISTRATION PHASE

In this section, we discussed the initialization phase, the way that system manager (SM) generated all security parameters, nodes identities ID_{SN}, ID_{SN}^{+}, ID_{HN}, ID_{FN}, and ID_{FN}^{+} to be later transferred in a secure channel. The steps are as follows:

1) The system manager (SM) generates a master key (K_{MS}), a secret unique identity for the sensor node ID_{SN}, an identity of first-level node ID_{FN}, and identity to hub node ID_{HN}.
2) The key is masked through

$$SK = h(K_{MS} \parallel ID_{SN} \parallel ID_{FN}) \qquad \textit{\textbf{Formula (1)}}$$

3) SM chooses a secret parameter l$*$ and adds it to the SK for pre-shared key confusion

$$PSK_n = l^* \oplus SK' \qquad \textit{\textbf{Formula (2)}}$$

4) SM produces a session sequence number for each session seq with size 32bit, and it is updated during each communication session. In the first session, the sequence number of all communicating parties selected by default.
5) Thus, the seq number becomes dynamic after the first successful session.
6) SM creates random number $q = \{q1, q2, q3, q_i\}$ to a generated masked ID_{SN} values in each session such $ID_{STi} = h(q_i \parallel SK' \parallel ID_{SN} \parallel seq \parallel l^*)$, so that

$$ID_{SN}^{+} = \{ID_{STi-2}, ID_{STi-1}, ID_{STi}\} \qquad \textit{\textbf{Formula (3)}}$$

This step is very important in the scheme because SM selects the proper ID to the legitimate sensor and stores those ID_{STi} in both legitimate sensor node and server node databases in a secure channel for the authentication process. Therefore, any intruder node had a different ID from the ID_{STi} stored in the database and sent any bogus request during the communication in the insecure channel is discarded by the HN as an illegitimate sensor.

SN→ $M_1 = \{\boldsymbol{SID_{new}}, \boldsymbol{X1}, \boldsymbol{t1}\}$	**←FN→** $M2 = \{\boldsymbol{SID_{new}}, \boldsymbol{a}, \boldsymbol{X1}, \boldsymbol{t1}, \boldsymbol{ID'_{FN}}\})$	**←HN** $((\boldsymbol{PSK^*_n}, \boldsymbol{ID^{++}_{FN}}, \boldsymbol{ID^{++}_{SN}}, \boldsymbol{ID^{+}_{FN}}, \boldsymbol{ID^{+}_{SN}}, \boldsymbol{seq^+}), \boldsymbol{t2})$
Generate t1 and random nonce rand Calculate, X1 X1= $PSK_n \oplus$ rand $\boldsymbol{X1 = PSK_n \oplus rand}$ ***Formula (5)*** $(\boldsymbol{SID_{new}}, \boldsymbol{X1}, \boldsymbol{t1})$ →	Add $ID'_{FN} = ID_{FN} \oplus ID_{HN}$ *Formula (6)* $(SID_{new}, X1, t1, ID'_{FN})$ →	Check the ID'_{FN} and the time validity $\Delta t = t2 - t1$ If $\Delta t = t2 - t1 > 0$ then continue, else abort the session. HN picks the correspond tuple from DB_{HN} $(PSK_n, ID^+_{FN}, ID^+_{SN}, ID_{FN}, ID_{SN}, seq)$ Calculate *SK'* from *Formula (1)* Calculate $l^* = PSK_n \oplus$ *SK'* from *Formula (2)* Deduce $rand = X1 \oplus PSK_n$ and calculate $SID_{new} = h\,(ID^+_{FN} \mid\mid ID^+_{SN} \mid\mid rand \mid\mid seq \mid\mid l^*)$ Deduce $X1^* = PSK_n \oplus rand$ from *Formula (5)* Check if $X1 \mathrel{?=} X1^*$ if successful continue Pick unique t2, seq^+, and nonce $rand^*$, and generate $ID^{++}_{FN} = ID_{SN}{}^{+} + \oplus rand^* \oplus ID^+_{FN}$, $SID_{new} = h\,(ID^{++}_{FN} \mid\mid ID^+_{SN} \mid\mid rand^* \mid\mid seq^+ \mid\mid t2)$ *Formula (7)* $SK^+ = h\,(K_{MS} \mid\mid SID_{new} \mid\mid ID^{++}_{FN})$ $ID^{++}_{SN} = h\,(rand^* \mid\mid SK^+ \mid\mid ID_{SN} \mid\mid l^* \mid\mid seq^+)$ $PSK_n^* = l^* \oplus SK+$ from *Formula (2)* Replace the tuple $NSK = (PSK^*_n, ID^{++}_{FN}, ID^{++}_{SN}, ID^+_{SN}, seq^+)$ Compute masking value to enable node from retrieving new session key parameters, $V1 = rand \oplus ID^{++}_{FN}, A = SID_{new} \oplus rand^*$ $B = seq^+ \oplus ID^{++}_{SN}$ *Formula (8)*
	Check the ID_{FN}' if it is the same as the stored in DB then proceed with session.	$(V1, A, B, t2, ID'_{FN})$ ←
Check the time validity $\boldsymbol{\Delta t = t3 - t2}$ Compute $\boldsymbol{ID^{++}_{FN} = rand \oplus V1}$ $\boldsymbol{rand^* = ID^{++}_{FN} \oplus ID^{+}_{FN} \oplus ID^{+}_{SN}}$ from ***Formula (7)*** $\boldsymbol{SID_{new} = rand^* \oplus A}$ from ***Formula (8)***, $\boldsymbol{seq^+ = h(ID^{++}_{FN} \parallel ID^{+}_{SN} \parallel rand^* \parallel SID_{new} \parallel t2)}$ from ***Formula (7)*** $\boldsymbol{SK^+ = h(K_{MS} \parallel SID_{new} \parallel ID^{++}_{FN})}$ from ***Formula (1)*** $\boldsymbol{ID^{++}_{SN} = B \oplus seq^+}$ from ***Formula (8)*** $\boldsymbol{PSK^*_n = l^* \oplus SK^+}$ from ***Formula (2)*** Replace the tuple $\boldsymbol{NSK = (PSK^*_n, ID^{++}_{FN}, ID^{++}_{SN}, ID^{+}_{SN}, seq^+)}$ and store session key.	$(V1, A, B, t2)$ ←	

FIGURE 2. P-I: Authentication and key agreement protocol.

7) The system creates an identity for FN to add more confusion to the shared parameters

$$ID^+_{FN} = ID_{SN} \oplus q_i \oplus ID_{FN} \qquad \textbf{\textit{Formula (4)}}$$

8) SM sends the parameter $(PSK_n, ID^+_{FN}, ID^+_{SN}, ID_{SN}, seq)$ to both the hub node and sensor node memories through a secure channel (local registration).
9) It Calculates $SID_{new} = h(ID^+_{FN} \parallel ID^+_{SN} \parallel rand \parallel l^* \parallel seq)$ and saves it as a default value to be shared for the first communication session between SN and HN.
10) The SM stores the ID_{SN}, ID_{FN}, and ID_{HN} in the SM memory.

B. P-I: AUTHENTICATION AND KEY AGREEMENT PHASE

In this section, we explained the centralized authentication protocol and the interaction between its entities to show the mutual authentication in our scheme between SN and HN through FN.

Furthermore, it contains four steps of interactions between sensor, first-level node, and hub node depicted in fig 2 and represented as follows:

Step1: SN → FN ($M_1 = \{SID_{new}, X1, t1\}$)

The sensor node generates current time *t1*, random nonce rand, and computes the following:

- Fetch the first new shadow identity for the sensor node SID_{new} for node anonymity, un-traceability, and privacy-preserving. Also, add a random nonce to the master key:

$$X1 = PSK_n \oplus rand \qquad \textbf{\textit{Formula (5)}}$$

- Transmit the tuples into the first level node FN with fresh parameters M1: $\{SID_{new}, X1, t1\}$.

  Step2:FN → HN ($M2 = \{SID_{new}, X1, t1, ID'_{FN}\}$)

  First level node FN gives extra protection to the data through masking the source of the message for anonymity, and un-traceability by creating a masked identity for FN through:

$$ID'_{FN} = ID_{FN} \oplus ID_{HN} \qquad \textbf{\textit{Formula (6)}}$$

- First level node FN adds its masked identity to the tuples M2: (SID_{new}, X1, t1, ID'_{FN}) and transfers the tuples to the hub node HN.

Step3: HN → FN (*M3= {V1, A, B, t2,*ID'_{FN}*}*)

Hub level node performs the following operations:

- Verify the $ID_{FN} = ID_{HN} \oplus ID'_{FN}$ from ***Formula (6)*** to initially authenticate FN and SN.
- Check the time validity $\Delta t = t2 - t1$ to avoid a replay attack.
- If $\Delta t = t2 - t1 > 0$ then continue, else abort the session.
- SN is not completely authenticated until HN picks the correspondent tuple from $DB_{HN}(PSK_n, ID^+_{FN}, ID^+_{SN}, ID_{FN}, ID_{SN}, seq)$ to verify the sensor identity ID_{SN}.
- Calculate master session key $SK = h(K_{MS}||ID_{SN}||ID_{FN})$ refer to ***Formula (1)***.
- Calculate the secure value generated by SM: $l^* = PSK_n \oplus SK$ we use ***Formula (2)***.
- Deduce the random nonce picked by the sensor $rand = X1 \oplus PSK_n$ refer to ***Formula (5)***.
- Calculate the hidden master key $X1^* = PSK_n \oplus rand$.
- Deduce sensor identity $SID_{new} = h(ID^+_{FN}||ID^+_{SN}||rand||seq||l^*)$ from Formula (3). This step is very important to verify the newly picked up sensor identity and use for the next masked identity generating. Whereas, the HN used $ID^+_{FN}, ID^+_{SN}, rand, seq$, and l the parameters stored in the DB to calculate the SID_{new} for the sensor and checked it with the parameters received from the FN.
- HN checks if the deduced $SID_{new} = SID_{new}$ sent from the request to validate the legitimate sensor and discards any malicious request from unidentified fake nodes with any different parameters $ID^+_{FN}, ID^+_{SN}, rand, seq$, and l.
- Check if $X1? = X1^*$ if successful continue, else abort the session.

When HN authenticates the sensor node, it performs the following:

- Pick fresh $t2$, unique seq^+, and nonce $rand^*$.
- Generate $ID^{++}_{FN} = ID^+_{SN} \oplus rand^* \oplus ID^+_{FN}$, $SID_{new} = h(ID^{++}_{FN}||ID^+_{SN}||rand^*||seq^+||t2)$,

$$SK^+ = h(K_{MS}||SID_{new}||ID^{++}_{FN}) \qquad \textbf{\textit{Formula (7)}}$$

- Update the new sensor identity to create SID_{new} for the next session:
  $ID^{++}_{SN} = h(rand^*||SK^+||ID_{SN}||l^*||seq^+)$, $PSK^*_n = l^* \oplus SK^+$ refer to ***Formula (2)***.
- Replace tuple $(PSK^*_n, ID^{++}_{FN}, ID^{++}_{SN}, ID^+_{FN}, ID^+_{SN}, seq^+)$ and store in the HN memory.
- Compute masking values to enable SN from retrieving new session parameters

$$V1 = rand \oplus ID^{++}_{FN}, \quad A = SID_{new} \oplus rand^*,$$
$$B = seq^+ \oplus ID^{++}_{SN} \qquad \textbf{\textit{Formula (8)}}$$

HN sends (V1, A, B, t2, $ID_{FN'}$) into FN to enable the first level node from authenticating that the message came from a legitimate source. FN drops the $ID_{FN'}$ from the tuples and directs them to the sensor node M4: (V1, A, B, t2).

Step4: FN → SN (*M4= {V1, A, B, t2}*)

After the SN receives the new parameters from FN, it performs the follows to get the new session key:

- Check the time validity $\Delta t = t3 - t2$ to avoid a replay attack.
- If $\Delta t = t3 - t2 > 0$ then continue, else abort the session.
- Compute the updated identity of the FN to be added into the new identity of the sensor node and random number for parameter confusion:
  $ID^{++}_{FN} = rand \oplus V1$, and $rand^* = ID^{++}_{FN} \oplus ID^+_{SN} \oplus ID^+_{FN}$ refer to ***Formula (7)***.
- Compute the shadow identity parameter, unique generated session sequence and insert it into new session key generation: $SID_{new} = rand^* \oplus A$, $seq^+ = h(ID^{++}_{FN}||ID^+_{SN}||rand^*|| SID_{new}||t2)$, and $SK^+ = h(K_{MS}||SID_{new}||ID^{++}_{FN})$ refer to ***Formula (7)***.
- Generate the new shadow identity for the next session of the SN, $ID^{++}_{SN} = B \oplus seq^+$ refer to ***Formula (8)***.
- Insert the parameter values to calculate the unique secret random number to obtain the new key:
  $PSK^*_n = l^* \oplus SK^+$ refer to ***Formula (2)***.
- Replace the tuple $(PSK^*_n, ID^{++}_{FN}, ID^{++}_{SN}, ID^+_{FN}, ID^+_{SN}, seq^+)$, store the session key, and use the new identity SID_{new} for the next communication session.
- Establish a secure connection.

C. P-II: RE-AUTHENTICATION PHASE

After a successful session of key agreement and authentication, the user is eligible to access the system components. The legitimate user might need to use the system and access some services during the day before midnight. Moreover, it is very inefficient, time-consuming, and energy-consuming to calculate all the parameters for the new session key where the user is already considered authorized. Therefore, the need for the concept of re-authentication arises to increase the system efficiency and reduce communication overhead, as depicted in fig 3. The steps of the re-authentication are as follows:

1) The user login to his/her account to access some information from the sensor.

Step1: SN → FN ($M_1 = \{SID_{new}, Xi, t1\}$)

- The sensor uses the last session key before midnight to authenticate the SN to the HN.

$$Xi = h(PSK_n \oplus SID_{new} \oplus rand) \qquad \textbf{\textit{Formula (9)}}$$

Step2:FN → HN (*M2=* {Xi, SID_{new}, *t1}*)

- FN only a forwarder.

Step3: HN → FN (*M3=* {L, t2})

- Check the time validity $\Delta t = t2 - t1 \Delta t = t2 - t1 > 0$ then continue, else abort the session.

SN→ $(M_1 = \{\boldsymbol{SID_{new}}, \boldsymbol{Xi}, \boldsymbol{t1}\})$	**←FN→** $(M2= \{\boldsymbol{SID_{new}}, \boldsymbol{Xi}, \boldsymbol{t1}\})$	**←HN** $(M3= \{\boldsymbol{L}, \boldsymbol{t2}\})$
Generate $\boldsymbol{t1}$ and use previous random nonce rand, and identity $\boldsymbol{SID_{new}}$, Calculate $\boldsymbol{Xi}$ $\boldsymbol{Xi = h\,(PSK_n \oplus SID_{new} \oplus rand)}$ ***Formula (9)*** $(\boldsymbol{Xi}, \boldsymbol{SID_{new}}, \boldsymbol{t1})$ →		
	Only a forwarder $(Xi, SID_{new}, t1)$ →	Check the time validity $\Delta t = t2 - t1$ If $\Delta t = t2 - t1 > 0$ then continue, else abort the session. HN check the SID_{new} was used during the last 12 hours. If it is then HN fetches the latest random number and calculates the new session key, $Xi^* = h\,(PSK_n \oplus SID_{new} \oplus rand)$ from ***Formula (9)*** Check if $Xi^* = Xi$ if successful continue Generate a new random number for the new session rand(i), where $i = \{i+1, i+2, i+3, i + n\,\|n{:}\ the\ number\ of\ new\ sessions\}$ $PSK_n^+ = h\,(rand\|\,\|PSK_n\,\|\,\|rand_{(i+1)})$ ***Formula (10)*** Generate current time and verify the HN acknowledgment $L = ID_{HN} \oplus ID_{SN}^{++} \oplus PSK_n^+$ ***Formula (11)*** Replace the tuple with the new session key $NSK = (PSK_n^+, ID_{FN}^{++}, ID_{SN}^{++}, ID_{SN}^{+}, seq^+)$. $(L, t2)$ ←
Check the time validity $\boldsymbol{\Delta t = t3 - t2}$ Check $\mathbf{PSK_n^+ = L \oplus ID_{SN}^{++} \oplus ID_{HN}}$ from ***Formula (11)*** Replace the tuple with the new session key $\boldsymbol{NSK = (PSK_n^+, ID_{FN}^{++}, ID_{SN}^{++}, ID_{SN}^{+}, seq^+)}$.	$(L, t2)$ ←	

FIGURE 3. P-II: Re-authentication protocol.

- HN checks if the SID_{new} was used during the last 12 hours. If it is, then HN fetches the latest random numbers, calculates the new session key: $Xi^* = h\,(PSK_n \oplus SID_{new} \oplus rand)$ from ***Formula (9)***.
- Check if $Xi^* = Xi$ to continue.
- Generate a new random number for the new session rand(i), where $i = \{i+1, i+2, i+3, i+n|n : the\ number\ of\ new\ sessions$, and use the latest two random numbers in the following formula:

$$PSK_n^+ = h(rand||PSK_n||rand_{(i+1)}) \qquad \textbf{\textit{Formula (10)}}$$

- Generate current time and verify the HN acknowledgment to the SN by calculating:

$$L = ID_{HN} \oplus ID_{SN}^{++} \oplus PSK_n^+ \qquad \textbf{\textit{Formula (11)}}$$

- Replace the tuple with the new session key $NSK = (PSK_n^+, ID_{FN}^{++}, ID_{SN}^{++}, ID_{SN}^{+}, seq^+)$.

Step4: FN → SN ($M4=$ {L, t2})

- Check the time validity $\Delta t = t3 - t2$, if $\Delta t = t3 - t2 > 0$ then continue, else abort the session.
- Check $PSK_n^+ = L \oplus ID_{SN}^{++} \oplus ID_{HN}$ from ***Formula (11)***.
- Replace the tuple with the new session key $NSK = (PSK_n^+, ID_{FN}^{++}, ID_{SN}^{++}, ID_{SN}^{+}, seq^+)$.
- A secure connection can be established between SN and HN.

D. EXPIRED KEY DELETION

The scheme generates a key deletion algorithm periodically to protect the system from any guessing attack attempt and clean its memories from unused expired keys. Moreover, this step is additional to [9] for security enhancement and reducing the chances of any possible malicious attack. The secure key deletion algorithm checks the valid keys along with the invalid keys in the SN/HN memory blocks and removes the invalid blocks from the system. Moreover, if the memory contains invalid blocks the system calculates the threshold value of valid/invalid blocks.

Consequently, the system checks the threshold results if the invalid blocks are more than the valid blocks, the system transfers the valid blocks to free space in the memory and delete the invalid keys [29]. The scheme used key derivation encryption (KDE) to encrypt the sensitive data and hierarchal tree structure to divide the keys and delete expired keys from the child node, as depicted in fig4. Their scheme used the AES 256bit key to encrypt the keys and keep them in the database.

IV. SECURITY ANALYSIS

In this section, we constructed a security analysis of our improved proposed protocols, their robustness against commonly known security attacks by using informal security analysis, as depicted in Table 2. Furthermore, we formally proofed the validity of the scheme by using BAN logic in the following sub-sections A and B.

A. FORMAL SCHEME PROOF WITH BAN LOGIC

In this sub-section, we used the well-known proof method BAN logic to confirm the scheme's mutual authentication and proper key agreement.

Basic notation:

The following contains the general basic notation for BAN logic to be used in both protocols P-I and P-II:

- $P| \equiv X$: P believes if X is true.
- $P \Delta X$: P sees X, i.e. someone sends a message containing X to P and P reads and repeats X.
- $P| \sim X$: P once said X, i.e. at some time P sent a message including X. It is not known if the message was sent recently or a long time ago, but it is known that P believes X then.
- $P| =\rangle\ X$: P controls X, i.e. P has authority over X and should be trusted on it.
- $\#(X)$: X is fresh, i.e. X has not previously been sent. $\bullet(X, Y)$:X or Y is one part of the formula (X, Y).
- $\langle X \rangle_Y$: X is combined with Y.
- $P \overset{K}{\longleftrightarrow} Q$: K is a secret parameter (to be) shared between P and Q.
- $P \overset{K}{\Longleftrightarrow} Q$: X is a secret parameter, which is known only to P and Q, and possibly to the parties trusted by them.
- $\frac{P}{Q}$: If P is true then Q is also true.

P-I Initial Assumptions:

The following contains the initial assumption for BAN logic to be used P-I:

A1: $HN| \equiv (SN \overset{ID_{SN}}{\longleftrightarrow} \mathrm{HN})$

A2: $HN| \equiv \#(t_n)$

A3: $HN |\equiv SN| \Longrightarrow (SN \overset{PSK_n}{\longleftrightarrow} HN)$

A4: $SN| \equiv | \equiv (SN \overset{ID_{SN}}{\longleftrightarrow} HN)$

A5: $SN| \equiv \#(rand*, seq+, tn)$

A6: $SN |\equiv HN| \Longrightarrow (SN \overset{NSK}{\longleftrightarrow} HN)$

Inference rules:

The following includes the general inference rule for BAN logic to be used in both protocols P-I and P-II:

- IR1 (Message-meaning rule): $\frac{\mathrm{P|\equiv P} \overset{Y}{\leftrightarrow} \mathrm{S,P\Delta\langle X\rangle}_Y}{\mathrm{P|\equiv S|\sim X}}$
- IR2 (Nonce-verification rule): $\frac{\mathrm{P|\equiv\#(X),P|\equiv S|\sim X}}{\mathrm{P|\equiv S|\equiv X}}$
- IR3 (Jurisdiction rule): $\frac{\mathrm{P|\equiv S}p\Rightarrow \mathrm{X,P|\equiv S|\equiv X}}{\mathrm{P|\equiv X}}$
- IR4 (Freshness rule): $\frac{\mathrm{P|\equiv\#(X)}}{\mathrm{P|\equiv\#(X,}Y)}$
- IR5 (Belief rule): $\frac{\mathrm{P|\equiv(X,}Y)}{\mathrm{P|\equiv X}}$

P-I Idealized form:

The following encompasses the idealized form for BAN logic to be used in P-I:

I1:$N \longrightarrow HN : (SN \overset{PSK_n}{\longleftrightarrow} HN, rand, seq, t)_{\mathrm{SN}} \overset{ID_{SN}}{\longleftrightarrow}_{\mathrm{HN}}$

I2:$HN \longrightarrow SN : (SN \overset{PSK_n}{\longleftrightarrow} HN, SK+, rand*, seq+, tn, SN \overset{NSK}{\longleftrightarrow} HN)_{\mathrm{SN}} \overset{ID_{SN}}{\longleftrightarrow}_{\mathrm{HN}}$

P-I Message in Idealized form:

The following comprises the message in idealized form for BAN logic to be used in P-I:

$M1 : SN \Rightarrow HN :\Rightarrow < SN \overset{rand}{\longleftrightarrow} HN, t1, seq, SID_{new}, X1 >$

$M2 : FN \Rightarrow HN :< FN \overset{ID'_{FN}}{\longleftrightarrow} HN, M1 >$

$M3 : HN \Rightarrow FN :< HN \overset{ID'_{FN}}{\longleftrightarrow} FN, V1, t2, A, B >$

$M4 : FN \Rightarrow SN : \ < FN \overset{NSK}{\longleftrightarrow} SN, M3 >$

P-I Goals:

The following includes the BAN logic goals of the in P-I:

$G1 : HN| \equiv SN \equiv (SN \overset{PSK_n}{\longleftrightarrow} HN)$

$G2 : HN| \equiv (SN \overset{PSK_n}{\longleftrightarrow} HN)$

$G3 : SN| \equiv HN \equiv (SN \overset{NSK}{\longleftrightarrow} HN)$

$G4 : SN| \equiv (SN \overset{NSK}{\longleftrightarrow} HN)$

P-I: Formal verification

Here we explain formal verification of the first protocol P-I.

Lemma 1: Message meaning rule: check to enable HN to verify the transmitted parameters from SN.

V1: From IR1, A1, and I1, as shown at the bottom of the next page:

Lemma 2: Freshness rule: HN checks whether the SN request is valid through Freshness rule.

V2: From IR4, A2, and I1 we get:

$$\frac{\mathrm{HN|\equiv\#(t_n)}}{\mathrm{HN|\equiv\#(SN\overset{PSK_n}{\longleftrightarrow}HN,rand,seq,t}_n)}$$

Lemma 3: Verification rule: HN verifies the SN request whether it is a legitimate sensor node or illegitimate.

V3: From V1, V2, and I1 we get, as shown at the bottom of the next page.

Lemma 4: Belief rule: HN now trusts SN and all its transmitted parameters.

V4: From V3, IR5 and I1 to accomplish G1:

$$\frac{\mathrm{HN|\equiv SN|\equiv(SN\overset{PSK_n}{\longleftrightarrow}HN,rand,tn,seq)}}{\mathrm{HN|\equiv SN|\equiv(SN\overset{PSK_n}{\longleftrightarrow}HN)}}$$

Lemma 5: Jurisdiction rule: now HN has a full control on the transmitted SN parameters.

V5: From A3, V4, IR3, and I1 we accomplish G2:

$$\frac{\mathrm{HN|\equiv SN{=}{>}(SN\overset{PSK_n}{\longleftrightarrow}HN).HN\ |\equiv SN|\equiv(SN\overset{PSK_n}{\longleftrightarrow}HN)}}{\mathrm{HN|\equiv(SN\overset{PSK_n}{\longleftrightarrow}HN)}}$$

Lemma 6: Message meaning rule: check to enable SN to verify the transmitted parameters from HN.

V6: From I2, A4, and IR1 we obtain, as shown at the bottom of the next page.

Lemma 7: Freshness rule: SN checks whether the HN request is valid through Freshness rule.

V7: From A2, P5, IR4 and I2 we obtain:

$$\frac{\mathrm{SN|\equiv\#(rand^*,seq^+,t_n)}}{\mathrm{SN|\equiv\#(PSK_n,SK^*,rand^*,seq^+,SN\overset{PSK_n^*}{\longleftrightarrow}HN)}}$$

Lemma 8: Verification rule: SN verifies the HN request whether it is a legitimate Hub node or illegitimate.

V8: From V7, V6, IR4, and I2 we get, as shown at the bottom of the next page.

Lemma 9: Belief rule: SN now trusts HN and all its transmitted parameters.

V9: From V8, IR5, and I2 we accomplish G3:

$$\frac{\mathrm{SN}|\equiv\mathrm{HN}|\equiv(\mathrm{PSK_n},\mathrm{SK}^*,\mathrm{rand}^*,\mathrm{t_n},\mathrm{seq}^+,\mathrm{SN}\overset{PSK_n^*}{\longleftrightarrow}\mathrm{HN})}{\mathrm{SN}|\equiv\mathrm{HN}|\equiv(\mathrm{SN}\overset{PSK_n^*}{\longleftrightarrow}\mathrm{HN})}$$

Lemma 10: Jurisdiction rule: now SN can obtain full parameters of the new session key from transmitted HN parameters.

V10: From A6, V9, IR3, and I2 we accomplish G4, as shown at the bottom of the page.

In summary, SN and HN achieve mutual authentication. In addition, based on Goal 1, Goal 2, Goal 3, and Goal 4, the session key SK securely shared between SN and HN.

In the following we verified the re-authentication protocol P-II for our scheme.

P-II Initial Assumptions

It is the same as P-I from A1- A4, and the change is in the following:

$$A5 : SN \ | \equiv \ \#(rand_{(i)}, t_n) A6 : SN \, | \equiv HN| \implies \left(SN \overset{PSK_n^+}{\longleftrightarrow} HN\right)$$

P-II Message in Idealized form:

The idealized form for BAN logic in P-II described as follows:

$M1 : SNHN :< S \Rightarrow N \overset{ID_{SN}}{\longleftrightarrow} HN, t1, SID_{new}, Xi >$

$M2 : FN \Rightarrow HN :< M1 >$

$M3 : HN \Rightarrow FN :< L, t2 >$

$M4 : FN \Rightarrow SN :< FN \overset{PSK_n^+}{\longleftrightarrow} SN, M3 >$

P-II Goals:

The BAN logic goals for P-II described as follows:

$G1 : HN| \equiv SN \equiv (SN \overset{PSK_n}{\longleftrightarrow} HN)$

$G2 : HN| \equiv (SN \overset{PSK_n}{\longleftrightarrow} HN)$

$G3 : SN| \equiv HN \equiv (SN \overset{PSK_n^+}{\longleftrightarrow} HN)$

$G4 : SN| \equiv (SN \overset{PSK_n^+}{\longleftrightarrow} HN)$

P-II: Formal verification

The BAN logic formal verification of P-II described as follows:

V1: From IR1, A1, and I1:

$$\frac{\mathrm{HN}|\equiv(\mathrm{SN}\overset{ID_{SN}}{\longleftrightarrow}\mathrm{HN}).\mathrm{HN}\nabla(\mathrm{SN}\overset{PSK_n}{\longleftrightarrow}\mathrm{HN},\mathrm{rand},\mathrm{tn},\mathrm{seq})_{\mathrm{N}\overset{ID_{SN}}{\longleftrightarrow}\mathrm{HN}}}{\mathrm{HN}|\equiv\mathrm{N}\sim(\mathrm{SN}\overset{PSK_n}{\longleftrightarrow}HN,t_n)}$$

V2: From IR4, A2, and I1:

$$\frac{\mathrm{HN}|\equiv\#(\mathrm{t_n})}{\mathrm{HN}|\equiv\#(\mathrm{SN}\overset{PSK_n}{\longleftrightarrow}\mathrm{HN},\mathrm{t_n})}$$

V3: From V1, V2, and I1:

$$\frac{\mathrm{HN}|\equiv\#(\mathrm{SN}\overset{PSK_n}{\longleftrightarrow}\mathrm{HN},\mathrm{tn}),\mathrm{HN}\ |\equiv\mathrm{N}\sim(\mathrm{SN}\overset{PSK_n}{\longleftrightarrow}\mathrm{HN},\mathrm{t_n})}{\mathrm{HN}|\equiv\mathrm{SN}|\equiv(\mathrm{SN}\overset{PSK_n}{\longleftrightarrow}\mathrm{HN},\mathrm{t_n})}$$

V4: From V3, IR5 and I1 to accomplish G1:

$$\frac{\mathrm{HN}|\equiv\mathrm{SN}|\equiv(\mathrm{SN}\overset{PSK_n}{\longleftrightarrow}\mathrm{HN},\mathrm{t_n})}{\mathrm{HN}|\equiv\mathrm{SN}|\equiv(\mathrm{SN}\overset{PSK_n}{\longleftrightarrow}\mathrm{HN})}$$

V5: From A3, V4, IR3, and I1 to accomplish G2:

$$\frac{\mathrm{HN}|\equiv\mathrm{SN}=>(\mathrm{SN}\overset{PSK_n}{\longleftrightarrow}\mathrm{HN}).\mathrm{HN}\ |\equiv\mathrm{SN}|\equiv(\mathrm{SN}\overset{PSK_n}{\longleftrightarrow}\mathrm{HN})}{\mathrm{HN}|\equiv(\mathrm{SN}\overset{PSK_n*}{\longleftrightarrow}\mathrm{HN})}$$

V6: From I2, A4, IR1, shown at the bottom of the next page.

V7: From A2, P5, IR4 and I2:

$$\frac{\mathrm{SN}|\equiv\#(\mathrm{rand},\mathrm{t}_n)}{\mathrm{SN}|\equiv\#(\mathrm{PSKn},\mathrm{PSKn}*,\mathrm{rand},\mathrm{SN}\overset{PSK_n*}{\longleftrightarrow}\mathrm{HN})}$$

V8: From V7, V6, IR4, and I2, as shown at the bottom of the next page.

V9: From V8, IR5, and I2 we accomplish G3:

$$\frac{\mathrm{SN}|\equiv\mathrm{HN}|\equiv(\mathrm{PSK}_n,\mathrm{PSK}_n^*,\mathrm{rand},\mathrm{tn},\mathrm{SN}\overset{PSK_n*}{\longleftrightarrow}\mathrm{HN})}{\mathrm{SN}|\equiv\mathrm{HN}|\equiv(\mathrm{SN}\overset{PSK_n^*}{\longleftrightarrow}\mathrm{HN})}$$

V10: From A6, V9, IR3, and I2 we accomplish G4, as shown at the bottom of the next page.

$$\frac{\mathrm{HN}| \equiv (\mathrm{SN} \overset{ID_{SN}}{\longleftrightarrow} \mathrm{HN}).\mathrm{HN}\nabla(\mathrm{SN} \overset{PSK_n}{\longleftrightarrow} \mathrm{HN, rand, tn, seq})_{\mathrm{N}\overset{ID_{SN}}{\longleftrightarrow}\mathrm{HN}}}{\mathrm{HN}| \equiv \mathrm{N} \sim (\mathrm{SN} \overset{PSK_n}{\longleftrightarrow} \mathrm{HN, rand, seq, t_n})}$$

$$\frac{\mathrm{HN}| \equiv \#(\mathrm{SN} \overset{PSK_n}{\longleftrightarrow} \mathrm{HN, rand, tn, seq}), \mathrm{HN} \mid \equiv \mathrm{N} \sim (\mathrm{SN} \overset{PSK_n}{\longleftrightarrow} \mathrm{HN, rand, tn, seq})}{\mathrm{HN}| \equiv \mathrm{SN}| \equiv (\mathrm{SN} \overset{PSK_n}{\longleftrightarrow} \mathrm{HN, rand, tn, seq})}$$

$$\frac{\mathrm{SN}| \equiv (\mathrm{HN} \overset{ID_{SN}}{\longleftrightarrow} \mathrm{SN}), \mathrm{SN}\ \nabla(\mathrm{PSK_n},\mathrm{SK}^*, \mathrm{rand}^*,\mathrm{seq}^+, \mathrm{t_n}, \mathrm{SN} \overset{PSK_n*}{\longleftrightarrow} \mathrm{HN})_{\mathrm{SN}\overset{ID_{SN}}{\longleftrightarrow}\mathrm{HN}}}{\mathrm{SN}| \equiv | \sim (\mathrm{PSK_n}, \mathrm{SK}^*, \mathrm{rand}^*,\mathrm{seq}^+, \mathrm{tn}, \mathrm{SN} \overset{PSK_n^*}{\longleftrightarrow} \mathrm{HN})}$$

$$\frac{\mathrm{SN}| \equiv \#(\mathrm{PSK_n}, \mathrm{SK}^*, \mathrm{rand}^*,\mathrm{t_n}, \mathrm{seq}^+, \mathrm{SN} \overset{PSK_n^*}{\longleftrightarrow} \mathrm{HN}, \mathrm{SN} \overset{ID_{SN}}{\longleftrightarrow} \mathrm{HN}).\mathrm{SN} \mid \equiv (\mathrm{PSK_n}, \mathrm{SK}^*, \mathrm{rand}^*,\mathrm{t_n}, \mathrm{seq}^+, \mathrm{SN} \overset{ID_{SN}}{\longleftrightarrow} \mathrm{HN})}{\mathrm{SN}| \equiv \mathrm{HN}| \equiv (\mathrm{PSK_n},\mathrm{SK}^*, \mathrm{rand}^*,\mathrm{seq}^+, \mathrm{SN} \overset{PSK_n^*}{\longleftrightarrow} \mathrm{HN})}$$

$$\frac{\mathrm{SN}| \equiv \mathrm{HN} => (\mathrm{SN} \overset{PSK_n^*}{\longleftrightarrow} \mathrm{HN}), \mathrm{SN} \mid \equiv \mathrm{HN}| \equiv (\mathrm{PSK_n}, \mathrm{SK}^*, \mathrm{rand}^*,\mathrm{t_n}, \mathrm{seq}^+, \mathrm{SN}\ \overset{PSK_n^*}{\longleftrightarrow} \mathrm{HN})}{\mathrm{SN}| \equiv (\mathrm{SN} \overset{PSK_n^*}{\longleftrightarrow} \mathrm{HN})}$$

From Goal 1, Goal 2, Goal 3, and Goal 4 it shows that the proposed protocol can achieve mutual authentication, and the session key SK is shared between SN and HN, according to above BAN logic analysis.

B. INFORMAL SECURITY ANALYSIS

The following list stated our system features:

1) MUTUAL AUTHENTICATION

In the authentication phase, the formulas are performed between the communicating nodes such as SN, HN, and the conduit between them FN. It ensures safe passage to the transmitted secured parameters in an insecure channel. Furthermore, we already conducted a BAN logic proof and it shows that our scheme can successfully achieve mutual authentication along with the key agreement between the communicated entities.

2) OFFLINE/ONLINE SECRET SHARED KEY GUESSING

The adversary A is capable of obtaining system information stored in SN or HN by using a successful combination of keys and ID credentials. Our scheme has a dynamic feature of refreshing along with protecting the sensor identity and session key by random values in both protocols. The scheme contains many randomized values and secret generated parameters such as secret unique value l^*, random nonce rand, session sequence number seq along with the strength of hash function to protect the main assets of the protocol. Also, our scheme applies secure key deletion which makes it very hard for the attacker to guess the key by getting access to the database.

3) NODES ANONYMITY

In the registration phase in section III, we indicated that the identity of the sensor ID_{SN} is masked through different random values and they are kept secret either by freshness or one-way hash function from *formula (3).* It is very hard for the attacker to guess the transmitted parameters in the unprotected channel. Since ID_{FN} and ID_{SN} are masked in their nodes before any transmission, it is very hard to obtain or track the source of the packet from SN or FN in the scheme in P-I. Once the sensor node masked identity SID_{new} is calculated in the initialization phase, it is constantly updated by HN in each new session in both protocols.

4) BRUTE FORCE ATTACK

Adversary A has a weak chance to launch a successful brute force attack due to the power of key length that adds time complexity to the system parameters. Moreover, our key size is adopting SHA-2 list of keys which is 224bit, so by estimating the time complexity to our hash key which is 2^{224}. Therefore, the attacker cannot lunch a successful guessing attack on our system hash function key or any parameter in polynomial time. The system's hash function key size is sufficient for the authentication operation. However, it can be increased when needed to meet security requirements in the future.

5) REPLAY ATTACK

While SN sends information to the server, it generates a timestamp t1 and computes: $SID_{new} = h(ID^{+}_{FN}||ID^{+}_{SN}||rand||seq)$ for the first session only then SID_{new} is updated by the HN. The adversary cannot obtain the real identity of the sensor ID_{SN} due to the complexity of the identity masking operation. The attacker needs to know ID_{SN}, besides that attacker cannot use an old generated identity in the current time. So, our scheme is robust against the replay attack.

6) INTEGRITY

The integrity of the message is protected in our scheme due to the power of the one-way hash function that exists in the master key during the initialization phase $SK = h(K_{MS}||ID_{SN}||ID_{FN})$. Moreover, it protects the identity generation during authentication phase in the sensor node $SID_{new} = h(ID^{+}_{FN}||ID^{+}_{SN}||rand||l*||seq)$ every communication session. Therefore, integrity is a fundamental part of our scheme along with privacy and anonymity.

$$\frac{\mathrm{SN}|\equiv(\mathrm{HN}\overset{ID_{SN}}{\longleftrightarrow}\mathrm{SN}),\ \mathrm{SN}\ \nabla(\mathrm{PSKn},\ \mathrm{PSKn}{*},\ \mathrm{rand},\ \mathrm{tn},\ \mathrm{SN}\ \overset{PSK_n*}{\longleftrightarrow}\ \mathrm{HN})_{\mathrm{SN}\overset{ID_{SN}}{\longleftrightarrow}\mathrm{HN}}}{\mathrm{SN}|\equiv|\sim(\mathrm{PSK_n},\mathrm{PSK_n}{*},\ \mathrm{rand},\mathrm{t_n},\ \mathrm{SN}\overset{PSK_n*}{\longleftrightarrow}\mathrm{HN})}$$

$$\frac{\mathrm{SN}|\equiv\#(\mathrm{PSK_n},\ \mathrm{PSK}^*_n,\ \mathrm{rand},\ \mathrm{tn},\ \mathrm{SN}\overset{PSK^*_n}{\longleftrightarrow}\mathrm{HN},\ \mathrm{SN}\overset{ID_{SN}}{\longleftrightarrow}\mathrm{HN}).\mathrm{SN}|\equiv(\mathrm{PSK_n},\mathrm{PSK_n}{*},\ \mathrm{rand},\ \mathrm{tn},\ \mathrm{SN}\ \overset{PSK^*_n}{\longleftrightarrow}\ \mathrm{HN})}{\mathrm{SN}|\equiv\mathrm{HN}|\equiv(\mathrm{PSK_n},\ \mathrm{P}SK^*_n,\ \mathrm{rand},\ \mathrm{SN}\overset{PSK_n*}{\longleftrightarrow}\mathrm{HN})}$$

$$\frac{\mathrm{SN}|\equiv\mathrm{HN}=>(\mathrm{SN}\overset{PSK^*_n}{\longleftrightarrow}\mathrm{HN}),\ \mathrm{SN}\ |\equiv\mathrm{HN}|\equiv(\mathrm{PSK_n},\ \mathrm{SK}^*,\ \mathrm{rand}^*,\ \mathrm{tn},\mathrm{seq}^+,\ \mathrm{SN}\overset{PSK^*_n}{\longleftrightarrow}\mathrm{HN})}{\mathrm{SN}|\equiv(\mathrm{SN}\overset{PSK^*_n}{\longleftrightarrow}\mathrm{HN})}$$

7) NODE IMPERSONATION

We assume that the adversary compromised an SN and got the tuple ID_{SN} stored in the sensor memory. At this point, the adversary cannot obtain any useful parameters that lead to knowing PSK_n of the HN, because PSK_n is protected by the one-way function h, a random nonce, and a secret unique parameter. Therefore, our scheme is robust against the impersonation attack.

8) SESSION HIJACKING ATTACK

Adversary A is capable of intercepting any message sent through an insecure communication channel. Moreover, the communicated parties SN, FN, and HN roam parameters among them. The adversary can obtain all the parameters transferred on both sides from SN to FN, from FN to HN, and on the way back. The attacker cannot successfully know the actual session key or the masked identity from parameters of the transmitted tuples $(SID_{new}, X1, t1)$ or $(V1, A, B, t2)$, because the parameters are protected by hash and fresh nonce random numbers. Moreover, when the attacker succeeds to gain a correct old session key used, the attacker cannot succeed in attacking the hub node because the HN checks the fresh identity of the sensor node. As a result, the scheme is secure against any possible session hijacking.

9) COLLISION ATTACK

Adversary A tries many combinations to break the hash function and obtains parameter values. This attack is impossible in our scheme because it is very hard to find two different messages that have the same value in hash function $h(m1) = h(m2)$. Thus, the strong hash function needs to avoid collision [30].Therefore, according to [28] the SHA-2 hash function family with key sizes: 224bit, 256bit, 384bit respectively is resistant to a collision attack.

10) SCALABILITY

Scalability is assured when the growth of the network by adding or removing a sensor or device will not affect the performance of the system. Our scheme is scalable in case of new node addition or unauthorized node discovery through registering each legitimate sensor node by the user with specific security parameters and IDs. Therefore, in any new communication, HN only allows the authentic sensor to join the session and discards illegitimate sensors. Moreover, according to [31], it necessitates reducing the computation overhead in WBANs communicating entities, to achieve scalability in the system. Therefore, the main aim of the paper is to improve the efficiency of [9] and we achieved our aim by reducing computation and communication overhead. Therefore, the proposed protocols achieve better scalability than other related schemes.

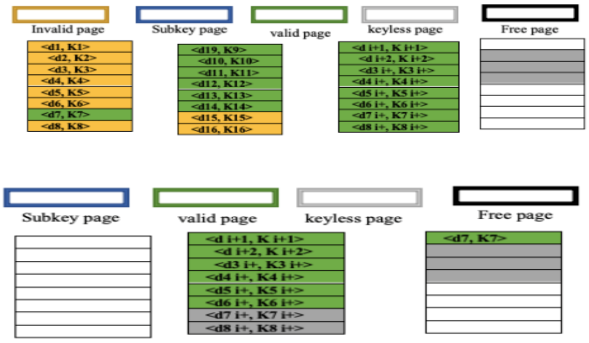

FIGURE 4. Key deletion scheme before and after using KDE [29].

11) FORWARD/BACKWARD SECRECY

Forward secrecy is the ability of the attacker to predict the future session key. While the backward secrecy occurs when the attacker collects as past session keys as possible to guess the previous session keys. In our proposed protocols, the session keys are dynamic and protected by different parameters such as random number, sequence number, new sensor identity, secret value, and the current time. So, even if the attacker guessed the session key correctly, he/she are not able to predict the future session key nor compromising the past session keys due to the complex parametric system. Moreover, the attacker needs to properly guess the following: $t2$,seq^{+}, $rand^{*}$, $ID_{FN}^{++} = ID_{SN}^{+} \oplus rand^{*} \oplus ID_{FN}^{+}$, $SID_{new} = h(ID_{FN}^{++} || ID_{SN}^{+} || rand^{*} || seq^{+} || t2)$, $SK^{+} = h(K_{MS} || SID_{new} || ID_{FN}^{++})$, and l^{*} to be able to penetrate the session and expose all the secret information. We have simulated our protocols by the Tamarin prover tool, and it showed that our scheme achieved forward secrecy. Therefore, this scheme is attaining perfect forward and backward secrecy.

V. PEFORMANCE ANALYSIS

In this section, we demonstrated the storage cost, communication overheads, and computational costs of our scheme.

A. COMPUTATIONAL COST

For the computational cost, the calculation was done for the authentication protocol based on, a one-way hash function that takes 0.06 ms based on the metrics in [9]. Our scheme computational cost is better than all other schemes in the sensor side [4], [9], [17], [18] with a 70% reduction by using P-I and 80% reduction by using P-II. Besides, P-I preforms similar to [9], [17], [18] in the hub node side, but better than [4], [25] and P-II performs better than all other schemes with an 80% reduction in the hub node side, as depicted in fig5. Furthermore, we chose a hash function with a 224bit key size to allow the sensor to have a sufficient amount of security more than [9], [17] which take a 160bit key size, and Koya and P. P [18] which takes a 128bit size key, (see Table 3 Table 4).

B. COMMUNICATION OVERHEAD

For calculating communication overhead, we assumed the length of the hash function, random number, updating foreign

TABLE 2. Comparison of our scheme computation cost.

Scheme	Xu et al.[4]	Kompara et al.[9]	Li et al.[17]	Koya and P. P [18]	Gupta et al.[25]	Ours P-I	P-II
Sensor	*5thash*	*3thash*	*3thash*	*3thash*	*7thash*	*2thash*	*1thash*
Hub	*7thash*	*5thash*	*5thash*	*5thash*	*10thash*	*5thash*	*2thash*

TABLE 3. Comparison of our scheme computation time.

Scheme	Xu et al.[4]	Kompara et al.[9]	Li et al.[17]	Koya and P. P [18]	Gupta et al.[25]	Ours P-I	P-II
Sensor	0.3 ms	0.18 ms	0.18 ms	0.18 ms	0.42 ms	0.12 ms	0.06 ms
Hub	0.42 ms	0.3 ms	0.3 ms	0.3 ms	0.6 ms	0.3 ms	0.12 ms

TABLE 4. Comparison of our scheme communication overhead.

Scheme	Xu et al.[4]	Kompara et al.[9]	Li et al.[17]	Koya and P. P [18]	Gupta et al.[25]	Ours P-I	P-II
Sensor	1280 bits	512 bits	672 bits	672 bits	1312 bits	480 bits	423 bits
Hub	768 bits	496 bits	656 bits	480 bits	1344 bits	704 bits	232 bits

TABLE 5. Comparison of our scheme security requirement.

Features	Xu et al.[4]	Kompara et al.[9]	Li et al.[17]	Koya and P. P [18]	Gupta et al.[25]	Ours
Offline/online shared secret guessing	×	-	×	×	×	✓
Anonymity	×	×	×	×	✓	✓
Brute force attack	✓	✓	×	×	✓	✓
FN-SN Replay attack	×	✓	×	×	✓	✓
SN/HN Impersonation	✓	✓	×	✓	✓	✓
Session hijacking	×	✓	×	×	×	✓
Expired Key deletion	×	×	×	×	×	✓
Integrity	✓	✓	✓	✓	✓	✓
Eavesdropping attack	✓	✓	×	✓	✓	✓
Re-authentication	×	×	×	×	×	✓
Collision Attack	×	✓	×	×	✓	✓

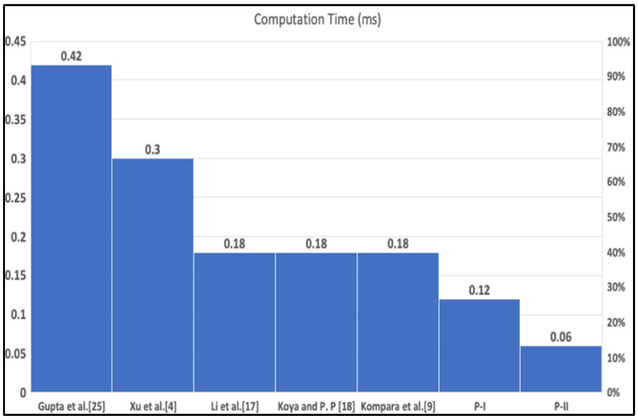

FIGURE 5. Computation time in the sensor.

network identity, masking sensor identity = 224bits, and the times along with session sequence number generation = 32bits respectively. Furthermore, our scheme contains three tuples in the sensor (SID_{new}, X1, t1) that results in =224+224+32= 480bit. Moreover, we have (V1, A, B, t2) from FN to SN that results in = 224+224+224+32 = 704bit. Those results show that our scheme has the least communication cost in the sensor side and performs better than all the schemes [4], [9], [17], [18], [25] with more robustness against various security attacks, as depicted in Table 5.

VI. CONCLUSION AND FUTURE WORK

In this work, we proposed lightweight anonymity preserving scheme for WBAN by applying the power of hash function and session key agreement. Our scheme is an enhancement to Kompara *et al.* [9] scheme by increasing the hash function key size and protecting the identity of all the communicating nodes. Moreover, the security analysis showed that P-II in our scheme has an 80% reduction of computation cost along with communication overhead and a higher resistance against brute force along with collision attacks. Hence, we proposed two points that have not been covered in the researches of the literature which are session key update and secure key deletion. Finally, a scheme formal proof was conducted using BAN logic to proof the mutual authentication. All in all, the future direction of the research will include scheme enhancement by using, lightweight key deletion scheme for the WBAN network along with a simulation through the Tamarin and Proverif tools.

REFERENCES

[1] G. K. Ragesh and K. Baskaran, "A survey on futuristic health care system: WBANs," *Procedia Eng.*, vol. 30, pp. 889–896, 2012, doi: 10.1016/j.proeng.2012.01.942.

[2] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Gener. Comput. Syst.*, vol. 78, pp. 659–676, Jan. 2018, doi: 10.1016/j.future.2017.04.036.

[3] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Comput. Electr. Eng.*, vol. 63, pp. 182–195, Oct. 2017, doi: 10.1016/j.compeleceng.2017.03.016.

[4] 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, doi: 10.1109/ACCESS.2019.2912870.

[5] B. A. Alzahrani, S. A. Chaudhry, A. Barnawi, A. Al-Barakati, and M. H. Alsharif, "A privacy preserving authentication scheme for roaming in IoT-based wireless mobile networks," *Symmetry*, vol. 12, no. 2, p. 287, Feb. 2020, doi: 10.3390/sym12020287.

[6] K. Sowjanya, M. Dasgupta, and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems," *Int. J. Inf. Secur.*, vol. 19, no. 1, pp. 129–146, Feb. 2020, doi: 10.1007/s10207-019-00464-9.

[7] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, "Efficient and secure anonymous authentication with location privacy for IoT-based WBANs," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2603–2611, Apr. 2020, doi: 10.1109/TII.2019.2925071.

[8] S. Deng, Z. Xiang, J. Yin, J. Taheri, and A. Y. Zomaya, "Composition-driven IoT service provisioning in distributed edges," *IEEE Access*, vol. 6, pp. 54258–54269, 2018, doi: 10.1109/ACCESS.2018.2871475.

[9] M. Kompara, S. H. Islam, and M. Hölbl, "A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs," *Comput. Netw.*, vol. 148, pp. 196–213, Jan. 2019, doi: 10.1016/j.comnet.2018.11.016.

[10] P. K. Sahoo, "Efficient security mechanisms for mHealth applications using wireless body sensor networks," *Sensors*, vol. 12, no. 9, pp. 12606–12633, Sep. 2012, doi: 10.3390/s120912606.

[11] F. Sulak, O. Koçak, E. Saygi, M. Ögünç, and B. Bozdemir, "A second pre-image attack and a collision attack to cryptographic hash function LUX," *Commun. Ser. A1 Math. Stat.*, vol. 66, no. 1, pp. 254–266, 2017, doi: 10.1501/Commua1_0000000794.

[12] G. Mehmood, M. Z. Khan, A. Waheed, M. Zareei, and 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, doi: 10.1109/ACCESS.2020.3007405.

[13] 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, Jun. 2020, doi: 10.1109/TCCN.2020.2982141.

[14] Y.-Y. Deng, C.-L. Chen, W.-J. Tsaur, Y.-W. Tang, and J.-H. Chen, "Internet of Things (IoT) based design of a secure and lightweight body area network (BAN) healthcare system," *Sensors*, vol. 17, no. 12, p. 2919, Dec. 2017, doi: 10.3390/s17122919.

[15] X. Liu, R. Zhang, and M. Zhao, "A robust authentication scheme with dynamic password for wireless body area networks," *Comput. Netw.*, vol. 161, pp. 220–234, Oct. 2019, doi: 10.1016/j.comnet.2019.07.003.

[16] A. Almuhaideb, B. Srinivasan, P. D. Le, M. Alhabeeb, and W. Alfehaid, "A hybrid mobile authentication model for ubiquitous networking," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 360–367, doi: 10.1109/Trustcom.2015.395.

[17] 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, Dec. 2017, doi: 10.1016/j.comnet.2017.03.013.

[18] A. M. Koya and P. P. Deepthi, "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network," *Comput. Netw.*, vol. 140, pp. 138–151, Jul. 2018, doi: 10.1016/j.comnet.2018.05.006.

[19] A. Arfaoui, A. Kribeche, and S.-M. Senouci, "Context-aware anonymous authentication protocols in the Internet of Things dedicated to e-health applications," *Comput. Netw.*, vol. 159, pp. 23–36, Aug. 2019, doi: 10.1016/j.comnet.2019.04.031.

[20] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *J. Netw. Comput. Appl.*, vol. 106, pp. 117–123, Mar. 2018, doi: 10.1016/j.jnca.2018.01.003.

[21] S. Deng, L. Huang, Y. Li, H. Zhou, Z. Wu, X. Cao, M. Y. Kataev, and L. Li, "Toward risk reduction for mobile service composition," *IEEE Trans. Cybern.*, vol. 46, no. 8, pp. 1807–1816, Aug. 2016, doi: 10.1109/TCYB.2015.2446443.

[22] Y. Lu, G. Xu, L. Li, and Y. Yang, "Robust privacy-preserving mutual authenticated key agreement scheme in roaming service for global mobility networks," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1454–1465, Jun. 2019, doi: 10.1109/JSYST.2018.2883349.

[23] V. Odelu, S. Saha, R. Prasath, L. Sadineni, M. Conti, and M. Jo, "Efficient privacy preserving device authentication in WBANs for industrial e-health applications," *Comput. Secur.*, vol. 83, pp. 300–312, Jun. 2019, doi: 10.1016/j.cose.2019.03.002.

[24] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K.-K.-R. Choo, and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 4, pp. 1310–1322, Jul. 2018, doi: 10.1109/JBHI.2017.2753464.

[25] 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, Jul. 2020, doi: 10.1016/j.comcom.2020.06.010.

[26] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K.-K.-R. Choo, "A robust and energy efficient authentication protocol for industrial Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1606–1615, Jun. 2018, doi: 10.1109/JIOT.2017.2787800.

[27] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 4, pp. 1299–1309, Jul. 2018, doi: 10.1109/JBHI.2017.2721545.

[28] M. Konan and W. Wang, "A secure mutual batch authentication scheme for patient data privacy preserving in WBAN," *Sensors*, vol. 19, no. 7, p. 1608, Apr. 2019, doi: 10.3390/s19071608.

[29] J. Xiong, L. Chen, M. Z. A. Bhuiyan, C. Cao, M. Wang, E. Luo, and X. Liu, "A secure data deletion scheme for IoT devices through key derivation encryption and data analysis," *Future Gener. Comput. Syst.*, vol. 111, pp. 741–753, Oct. 2020, doi: 10.1016/j.future.2019.10.017.

[30] A. Braeken, "Highly efficient symmetric key based authentication and key agreement protocol using Keccak," *Sensors*, vol. 20, no. 8, p. 2160, Apr. 2020, doi: 10.3390/s20082160.

[31] M. E. S. Saeed, Q.-Y. Liu, G. Tian, B. Gao, and F. Li, "Remote authentication schemes for wireless body area networks based on the Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4926–4944, Dec. 2018, doi: 10.1109/JIOT.2018.2876133.

ABDULLAH M. ALMUHAIDEB received the B.S. degree (Hons.) in computer information system from King Faisal University, Saudi Arabia, in 2003, and the M.S. (Hons.) and Ph.D. degrees in network security from Monash University, Melbourne, Australia, in 2007 and 2013, respectively. He is currently an Assistant Professor of Information Security and the Dean of the College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Saudi Arabia. He has published more than 25 scientific articles in journals and premier ACM/IEEE/Springer conferences, such as TrustCom, NCA, MobiQuitous, ICICS, and AINA. His research interests include mobile security, authentication and identification, and ubiquitous wireless access.

KAWTHER S. ALQUDAIHI received the bachelor's degree in computer science from Jubail University College, in 2013. She is currently pursuing the M.Sc. degree with Imam Abdulrahman Bin Faisal University. She is also a Researcher with Imam Abdulrahman Bin Faisal University. Her research interests include cryptography, wireless body area networks, information security, and secure communication protocols.