Received April 21, 2021, accepted May 14, 2021, date of publication May 25, 2021, date of current version June 4, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3083708

An Improved WBSN Key-Agreement Protocol Based on Static Parameters and Hash Functions

BEHROOZ KHADEM[1], AMIN MASOUMI SUTEH[1], MUSHEER AHMAD[2], AHMED ALKHAYYAT[3], MOHAMMAD SABZINEJAD FARASH[4], AND HANY S. KHALIFA[5]

[1]Information Technology and Communication Faculty, Imam Hossein University, Tehran 1698715461, Iran
[2]Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India
[3]Department of Computer Technical Engineering, College of Technical Engineering, Islamic University, Najaf 192122, Iraq
[4]Faculty of Mathematical Sciences and Computer, Kharazmi University, Tehran, Iran
[5]Department of Computer Science, Misr Higher Institute of Commerce and Computers, Mansoura 35511, Egypt

Corresponding author: Musheer Ahmad (musheer.cse@gmail.com)

ABSTRACT Wireless telecommunications systems have expanded rapidly over the past few years. Wireless Body Sensor Network (WBSN) is a relatively novel area of research and development in healthcare systems. However, it has multiple constraints and challenges regarding human health, social interactions, coverage radius, energy consumption, and communication reliability. In addition, communications between nodes can contain highly sensitive personal information, while hostile environments will impose a wide range of security risks. Therefore, designing authenticated key agreement (AKA) protocols is a crucial challenge in these networks. The current study, considering the security issues of the Li *et al.* scheme and some of their new extensions, proposes an improved AKA protocol with anonymity and unlinkability of the sensor node sessions. The results of theoretical analysis compared with similar schemes indicated that the proposed scheme could reduce average energy consumption and communication cost by 41 percent. It also reduced the average computation time by 61 percent. Furthermore, it was shown by formal/informal analyses that, on top of unlinkability and anonymity features, other central security features in the current scheme were similar and comparable to those in the recent and similar schemes.

INDEX TERMS Authentication, anonymity, formal verification, unlinkability, wireless body sensor network.

I. INTRODUCTION

The infrastructural weaknesses, uncontrollable environments, and the nature of wireless communications have brought about multiple information security challenges for WBSN. Since guaranteeing a secure link in the session initiation protocol necessitates a secure mutual authenticated key agreement (AKA) to secure further communications, in the last decade, the lightweight authentication and key-agreement mechanism have been addressed by several studies.

AKA allows the server in WBSN to verify the user ID when accessing the system and attempting to generate a session key. Hence, in these networks using key-agreement protocols to generate a session key between the sensor node and the hub node is a promising solution to counter the threats and improve security. However, providing such schemes with sensor node anonymity and session unlinkability has recently become a challenge. This gap is one of the primary motives behind the current research.

WBSN offers many advantages that make it attractive for researchers and industries [1]. As such, WBSN has been proposed to facilitate an effective paradigm for e-health and telemedicine requirements [2]. Miniature sensor nodes on the body (wearable) or inside the body (implantable) allow dynamic monitoring of the physiological information such as blood pressure, heart rate, and body temperature without interfering with daily activities [3].

Especially recently, the coronavirus disease 2019 (COVID-19) has caused unprecedented restrictions in social activities, along with the loss of lives, economic chaos, and disruption of humanitarian aid. Despite the advance of technological developments, research activities have shown that several issues need further investigation for optimal response to the COVID-19 pandemic. Upon the COVID-19 outbreak, governments and organizations have decided to

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

home treatment of the mild illness patients as a precautionary measure to reduce the risk of contagion [4].

Therefore, the application of WBSN can be an effective response to these new challenges. The main goal of this approach is monitoring, which includes tracking and recording the vital and significant changes in the health of patients [5].

After introducing the IEEE Standard 802.15.6 (WBAN) in 2012 [6], as a promising wireless technology for low-power devices, numerous cryptography protocols were proposed based on sensitivity, universality, and mobility of the network [7].

Toorani (2016) analyzed the security of the IEEE 802.15.6-2012 standard. He pointed out that some protocols had minor weaknesses that made them vulnerable to various attacks. He also noted that such minor vulnerabilities, which were linked to the safety regulations in the standard, could be particularly important in medical fields that deal with patients' confidential and sensitive information and could be a threat to human life [8].

In another report, Ibrahim *et al.* (2016) proposed a lightweight and efficient mechanism for a mutual authenticated key agreement based on the anonymity and unlinkability of the sensor node [9]. Their solution was highly efficient for recourse-constrained sensors as it only employed hash and XOR computations instead of elliptic curve cryptography [10]–[14].

Later, Li *et al.* (2017) introduced an improved solution in the two-hop network [15]. Their scheme started via predeployed keys and parameters by the system administrator and after the mutual authentication of the nodes, a new session key was generated. The solution primarily aimed to decrease the cost of complexity by maintaining the anonymity and unlinkability of the sensor node during the protocol execution.

Yeh *et al.* (2016) presented a secure (Internet of Things) IoT-based healthcare protocol that worked through the body sensor network. To simultaneously achieve system performance and transmission robustness in public IoT-based networks, they used robust cryptography primitives to build two communication mechanisms to ensure confidentiality of transmission and authentication among smart nodes, processing units, and supporting BSN servers. In addition, they implemented the proposed healthcare system with the Raspberry PI platform to explain its feasibility.

On the other hand, based on the latest standards and publications, Al-Janabi *et al.* (2017) examined the WBSN communication architecture model, their related attacks, privacy requirements, and some of the main challenges of WBSNs. The study also involved some security measures and advanced research in WBSN and was concluded by pointing out some open problems and future research gaps [19].

Likewise, Salayma *et al.* (2017) performed a survey on WBSN. This review placed considerable emphasis on the main concept and features of WBSN technology. First, the concept of WBSN was introduced and an overview of the key applications offered by this network technology was introduced. Then this study examined a wide range of communication standards and methods used in WBSN. Due to the sensitivity of the information operated by the WBSN, fault tolerance is an important issue and was widely discussed. In addition, this review thoroughly examines the fault tolerance and reliability paradigms proposed for WBSN. Challenging and open research topics related to fault tolerance, coexistence and power consumption, and interference management were also discussed, while future trends in these aspects were proposed [20].

Li *et al.* (2018) presented a successful differential fault analysis for breaking three versions of the PHOTON protocol family. Using mathematical analyses and simulation of experimental results, they showed that in order to retrieve each message input for PHOTON-224/32/32, PHOTON-160/36/36, and PHOTON-80/16/16, on average 86, 69, and 33 random errors were required, respectively. This was PHOTON's first failure using the Differential Fault Analysis method, which provided a new reference for security analysis of other similar structures in WBSN [21].

Khan *et al.* (2018) covered the latest advancements with some discussion on the available radio technologies for WBSN. In their research, some future trends and challenges in this area were discussed [22].

Kumar *et al.* (2018) reviewed a mutual authentication protocol for telemedicine information schemes in the cloud computing environment designed by Mohit *et al.* and found that it was vulnerable to stolen verifier attacks. Moreover, it did not perform desirably for the patient anonymity and against the patient attack and forgery attack and failed to protect the key session. To increase security, they introduced a novel authentication protocol, which was also better in terms of time calculation cost. Furthermore, the protocol security assessment protected the flexibility of all possible security features, while they also conducted a formal security assessment based on the random oracle model. Finally, the authors displayed that the performance of the proposed protocol was significantly higher than some of the existing protocols [23].

Ali et al (2018) investigated a user authentication scheme for an e-healthcare scheme and found some weaknesses such as password guessing, identity guessing attacks, user impersonation, attack on smart card theft, premium insider attack, and attack on smart card theft. To strengthen the scheme and improve security, they developed a remote biometric-based user authentication protocol. The proposed design was checked by BAN logic and a valid randomized model. Informal security analysis illustrated that the proposal was secure against malicious attacks. Also, the proposed scheme was simulated with AVISPA, and the simulation results showed that it was secure against passive and active attacks. The proposed protocol was then compared with some other protocols in terms of evaluation parameters such as time calculation cost, storage cost, communication cost, and estimated time [24].

Kompara *et al.* (2019) analyzed an existing key-agreement protocol. They discovered some weaknesses in the scheme security. To improve security and prevent the attacker from draining the limited resources available or gaining access, they designed a new key-agreement protocol that was based on the previous protocol. Their new design provided higher security while maintaining comparable energy consumption [25].

Alzahrani *et al.* (2020) showed that one of the latest WBSN-based authentication schemes was prone to session key recovery attacks, key compromise impersonation, and temporary session-specific information attacks. Furthermore, they presented a WBSN anonymous authenticated key exchange (AKE) scheme with better efficiency and security to show the known weaknesses in the previous scheme. In addition, they formally and informally evaluated the performance of the proposed protocol using the ProVerif automated tool and the random oracle model. Results indicated that the protocol not only was efficient but could also provide robust and implementable security features [26].

Tanveer *et al.* (2020) introduced a new lightweight AKE protocol for the UAV internet environment (LAKE-IoD), which ensured mobile user authentication and the mechanism for creating session keys between UAVs and mobile users. The LAKE-IoD scheme was an AKE protocol based on the AEGIS program, XOR, and hash. Accurate formal security verification Use of Scyther and informal security showed that LAKE-IoD was secure against some known attacks. Furthermore, the BAN logic was used to verify the logical completeness of LAKE-IoD. Also, comparing LAKE-IoD with related designs, they showed that LAKE-IoD used less communication, computing, and overhead storage [28].

Tanveer *et al.* (2020) presented an authentication scheme for 6LoWPAN (LAS-6LE) environments. The LAS-6LE first verified the accuracy of the SN transmission data, then considered a secret key for the server and the SN to perform access to the information. The logical accuracy of the LAS-6LE was verified by the BAN logic. They showed that the LAS-6LE in the 6LoWPAN environment consumed fewer resources than other similar designs [29].

Chen *et al.* (2018) rejected the unlinkability feature between sessions that was claimed by Li *et al.* and instead, proposed an improved scheme by adding a predefined parameter and hash functions [30]. In addition, Khan *et al.* (2018) cast doubt on the anonymity of Li's protocol [31]. The authors proposed an improved scheme by employing the additional hash functions and an auxiliary parameter for mutual authentication, however, their scheme increased computational complexity. Recently, Kompara *et al.* (2019) could improve it to a low-complexity robust scheme. They showed that Li's scheme required session unlinkability and protocol structural integrity, as well as higher security against threats such as jamming [32].

TABLE 1. Symbols and abbreviations.

Symbol	Description
SA	System Administrator
N	First Level node-Sensor Node
IN	Second Level Node/Intermediate Node
HN	Hub Node
id_N	Identity of SN
id'_{IN}	Short identity of First level sensor node
K_{HN}	Secret key of Hub Node
K_N	Secret key-parameter of Sensor Node
r_N, r_H	Temporary secret parameters as a nonce
a_N, b_N	Authentication parameters
m_1, m_2, m_3, m_4	Auxiliary parameters required for authentication
t_N, t_H	Timestamp generated by SN-HN
t_c, t'_c	Constant message received time
k_S	Session Key to be agreed upon
h(.)	one-way hash with Collision-resistant property
$\|\|$	Concatenation
$\oplus$	Bitwise XOR
$X \rightarrow Y : M$	Entity X transmit the message M to entity Y via a public channel

A. ABBREVIATIONS AND ACRONYMS

The SN is assumed as the second-level node and contacts the HN via the intermediate node (IN). If the SN is assumed as the first level node, the scheme can be adapted to direct communication with the HN. Table 1 shows the symbols and abbreviations used in this paper.

In this paper, h:$\{0, 1\}^*$ $\longrightarrow$ $\{0, 1\}^t$ is also assumed as a powerful hash function.

II. MOTIVATIONS AND CONTRIBUTIONS

Despite introducing some improved schemes, there are still limitations in WBSN communications. Therefore, based on the reviewed schemes above, the current study attempted to propose a lightweight scheme suitable for two-hop or two-tier centralized WBSN. One of the key characteristics of sensor nodes in wireless networks is their passive mode, which is tied to the protocol design. Accordingly, we aimed at reducing the online/live statement in a special period or reducing the channel rate to run an efficient key agreement protocol. Therefore, in the present paper, when we discuss the nature of the sensors, it means that the sensor node does not need to be always active/present/online to create a new session key. The contributions of this paper are as follows:

1) Optimizing protocol structure via refreshing the auxiliary authentication parameters at the beginning of each session without the requirement to update the pre-deployed parameters to decrease waiting-time;
2) Unlinkability between the subsequent sessions of a sensor node according to the anonymity;
3) Validating the security of the new scheme via official (formal) and non-official proofing;

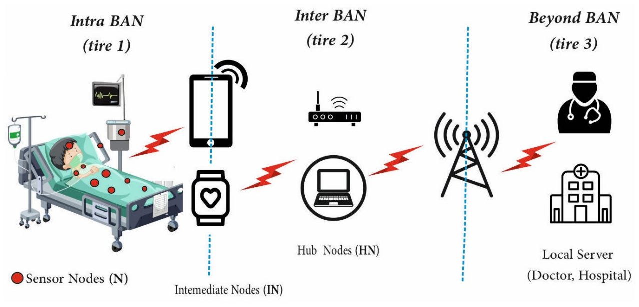


FIGURE 1. Three-tire WBSN network architecture.

4) Reducing the computational complexity, energy consumption, and transmission bandwidth of the network.

This article is organized as follows: Section III discusses the system model. Section IV presents the proposed scheme, and Section V analyzes conventional security attributes. Next, Section VI presents a formal verification of the scheme using the Scyther tool. In Section VII by evaluating the efficiency of the proposed scheme and comparing it with a previous scheme, its computational and communication costs and energy consumption are discussed. Finally, the conclusion is given in Section VIII.

III. THE SYSTEM MODEL

Figure 1 illustrates how the general WBSN architecture can be classified into a three-tier architecture [33], [34].

1) Tier-1 (Intra-BAN): consists of physical sensor nodes and personal servers (i.e. a smartphone or smartwatch).
2) Tier-2 (Inter-BAN): a layer that adds an access point to the network, in a way that the personal server connects and routes to other wireless networks.
3) Tier-3 (Beyond-BAN): consists of other wireless or public area networks that transmit the collected data to the caregiver terminal database (CT).

The centralized two-hop or two-tier network proposed by Li *et al.* consists of three node types (Figure 2):

1) SN or N: the second-level node (i.e. the sensor node implanted in the body). These nodes, due to resource constraints, usually have limited computational and communicational power.
2) FN or IN: the first-level node that can also be referred to as the intermediate or coordinator node (i.e. smartphone or smartwatch) which has a higher computational and communicational power and storage, compared with the SN.
3) HN: the hub node or a local server (e.g. personal computer). This node has higher computational power and resources than others. Hub nodes are assumed to be always in the range of INs.

The HN and IN are the intermediate parts of the body sensor network and occupy the second level of the network. The link between the IN and SN is the internal part and is assumed as the first network level. Note that HN is outside the coverage area of SN, therefore immediately after monitoring and collecting vital signals, SNs in the internal part send the vitals of the patient to the HN via the IN.

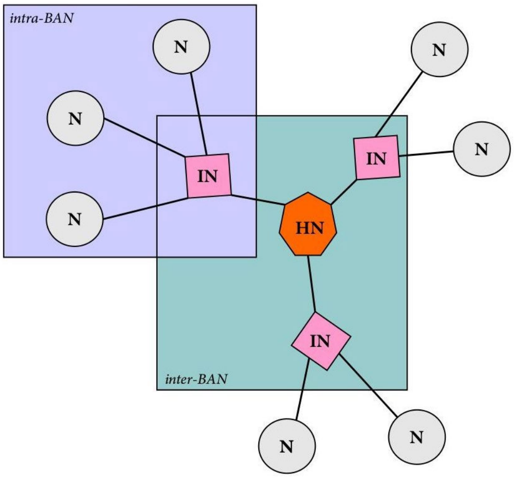


FIGURE 2. Two-tire WBSN model.

The HN retains patients' authentication data and processes them after collecting the vital signals from the internal part. Then, based on the priority of critical information, HN transmits the signals to medical service servers.

In the scheme of Li *et al.*, the security prerequisites follow the Dolev-Yao threat model [35]. We also followed the same model in our proposed protocol. In the Dolev-Yao threat model, the communication between two entities is accomplished over a public (open) channel, and an adversary will have full control over the communication channel. Therefore, the adversary can alter, eavesdrop, insert, and delete forgery messages that are transmitted during the communication. In addition, it is assumed that the adversary can physically capture one or more sensing nodes in the network and can steal all sensitive information stored in the captured sensing nodes which utilize the strength analysis attacks. In our proposed protocol, we follow the Dolev-Yao threat model. Furthermore, the HN is assumed trustable in the current study; nevertheless, the adversary may penetrate the HN database and tamper with or steal the data. Note that only the master key of the HN is assumed completely inaccessible to the adversary. Also, any SN may be captured, meaning that the adversary can extract the secret information stored in the sensor memory. Thus, we use the threat model utilized in Li *et al.* scheme, too.

IV. THE PROPOSED PROTOCOL SCHEME

Similar to previous schemes [9], [15], [30]–[32], the proposed scheme consists of three phases; the initialization and registration phases are performed by the system administrator in a secure environment, whereas the authentication phase is conducted in a public channel using a new idea.

A. INITIALIZATION PHASE

In this phase, the system administrator initializes the hub node HN and assigns a master key K_{HN} to HN. Then the administrator stores K_{HN} in the HN memory.

B. REGISTRATION PHASE

In this phase, first the system administrator registers the sensor node by devoting a unique ID (called id_N) and a secret parameter (K_N) generated for the SN in the network. Then Eq. (1) and (2) are computed and the tuple $< id_N, a_N, b_N >$ is stored in the SN memory.

$$a_N = h(id_N \parallel K_N) \tag{1}$$
$$b_N = K_{HN} \oplus K_N \oplus id_N \tag{2}$$

Finally, a table containing all K_N values assigned to the nodes as well as all a_N values computed by the corresponding K_N is stored in the HN memory. If there is an IN in the network, SA picks a short unique ID (called id'_{IN}) and stores it in IN memory. The id'_{IN} is also stored in the HN memory. Note that, the K_{HN} from the previous phase is already stored in the HN and therefore, the tuple $< id'_{IN}, K_{HN}, T(K_{Ni}, a_{Ni}) >$ is stored in the HN memory.

C. AUTHENTICATION AND SESSION KEY AGREEMENT PHASE

In the authentication phase, SN attempts for an agreement on the session key (K_S) as an anonymous mutual authentication with the HN (Figure 3).

Step 1: $SN \rightarrow IN :< m_1, m_2, t_N >$. The SN generates a timestamp t_N and a temporary secret parameter r_N as a nonce. Then it computes authentication parameters (Eq. 3 and 4) and sends the tuple $< m_1, m_2, t_N >$ to the IN.

$$m_1 = a_N \oplus r_N \tag{3}$$
$$m_2 = ((id_N \oplus b_N) \parallel t_N) \oplus (t_N \parallel r_N) \tag{4}$$

Step 2: $IN \rightarrow HN :< m_1, m_2, t_N, id'_{IN} >$. The IN adds its own ID (id'_{IN}) to the received message without changing the message, and then transmits the tuple $< m_1, m_2, t_N, id'_{IN} >$ to the HN.

Step 3: $HN \rightarrow IN :< m_3, m_4, t_H, id'_{IN} >$. First the HN checks and verifies id'_{IN} based on the value it has stored in its memory. Then it verifies the timestamp t_N via the default validation (Eq. 5), where t_C and Δt denote the reception time of the message and the maximum transmission delay, respectively. If authentication fails, the protocol execution halts. The condition for security is also defined as follows: Δt is smaller than the minimum attack time $t_{min}(\Delta t < t)$.

$$|t_C - t_N| \overset{?}{<} \Delta t \tag{5}$$

After verifying the received data, HN has to check and compute Eq. (6) for authenticating the SN.

$$m_2 \oplus (K_{HN} \parallel t_N) \overset{?}{=} (K_N \parallel (0)^{32}) \oplus (t_N \oplus (a_N \parallel m_1)) \tag{6}$$

Therefore, HN has to search in the stored table $T(K_{Ni}, a_{Ni})$ and check for correct (K_N, a_N) pairs for Eq. (7). If the correct (K_N, a_N) pair is not found, authentication fails. After verification and successful authentication, the timestamp t_H is generated and the temporary secret parameter r_H will be picked by the HN. Then Eq. (7) and authentication auxiliary parameters Eq. (8) and (9) will be computed for mutual authentication.

$$r_N = m_1 \oplus a_N \tag{7}$$
$$m_3 = a_N \oplus r_H \tag{8}$$
$$m_4 = K_{HN} \oplus K_N \oplus h(a_N \parallel r_N \parallel r_H) \tag{9}$$

Then, the new session key (Eq. 10) will be generated and stored. At the end of this step, the tuple $< m_3, m_4, t_H, id_{IN} >$ will be transmitted to the IN.

$$K_s = h(m_1 \parallel r_N \parallel a_N \parallel r_H \parallel t_N \parallel m_4 \parallel t_H) \tag{10}$$

Step 4: $IN \rightarrow SN :< m_3, m_4, t_H >$. Here the IN acquires its ID (id_{IN}) and if the ID is validated, the rest of the received message $< m_3, m_4, t_H >$ will be sent to the SN.

Step 5: . N. The SN receives the tuple $< m_3, m_4, t_H >$ and verifies the timestamp t_H. Then, it computes Eq. (12) and verifies Eq. (13).

$$|t_C - t_H| \overset{?}{<} \Delta t \tag{11}$$
$$r_H = m_3 \oplus a_N \tag{12}$$

If Eq. (13) is not satisfied, the authentication phase will fail and the SN will retry the protocol execution. Therefore, after mutual authentication, the session key (Eq. 14) will be computed and stored in its memory to be used in the next communications.

$$m_4 \oplus id_N \oplus b_N \overset{?}{=} h(a_N \parallel r_N \parallel r_H) \tag{13}$$
$$K_s = h(m_1 \parallel r_N \parallel a_N \parallel r_H \parallel t_N \parallel m_4 \parallel t_H) \tag{14}$$

V. SECURITY ANALYSIS OF THE PROPOSED PROTOCOL

In this section, some of the common WBSN attacks along with the security of our proposed scheme against these attacks will be discussed.

A. ANONYMITY AND SESSION UNLINKABILITY

We showed in the proposed scheme that even in the case of observing all communications via the protocol, the adversary could not learn the ID of any SN, because id_N was not transmitted in the public channel. Parameter m_1 has the value a_N and id_N that are protected by the one-way resistant hash function in Eq. (1).

Further, the ID in m_2 is combined with temporary random parameters r_N, t_N, and the secret k_N, as well as the k_{HN} secret key.

In addition, because m_1 and m_2 values are refreshed by fresh secret random parameters in each session, the adversary cannot link a session with another successfully completed session of the same SN. Unlinkability is a more outstanding feature than anonymity, which protects the generation process of a session key in the protocol from leading to tracing the corresponding SN of the session.

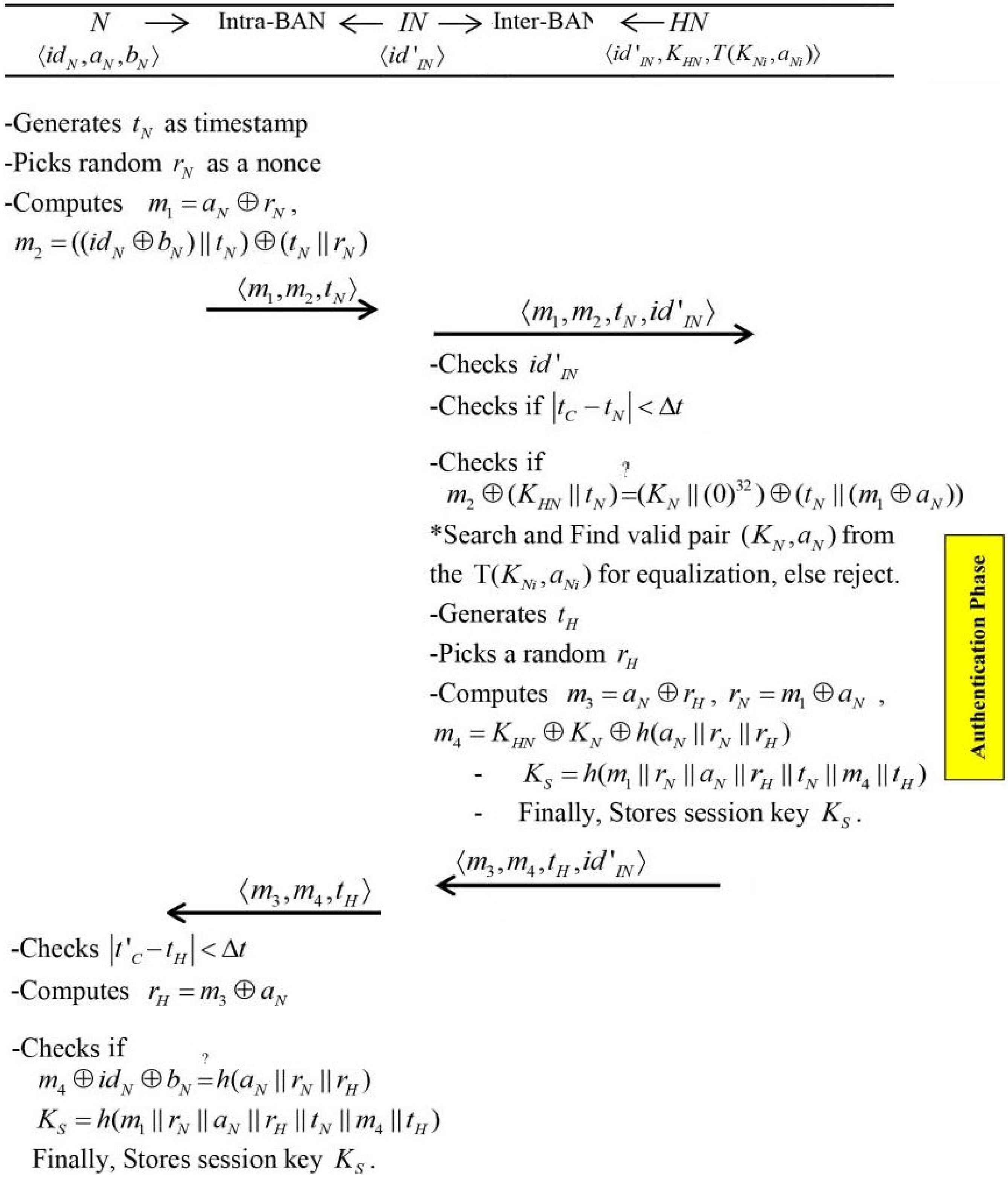

$N \longrightarrow$ Intra-BAN $\longleftarrow IN \longrightarrow$ Inter-BAN $\longleftarrow HN$
$\langle id_N, a_N, b_N \rangle$
$\langle id'_{IN} \rangle$
$\langle id'_{IN}, K_{HN}, T(K_{Ni}, a_{Ni}) \rangle$
-Generates t_N as timestamp
-Picks random r_N as a nonce
-Computes $m_1 = a_N \oplus r_N$,
$m_2 = ((id_N \oplus b_N) \| t_N) \oplus (t_N \| r_N)$
$\langle m_1, m_2, t_N \rangle$
$\langle m_1, m_2, t_N, id'_{IN} \rangle$
-Checks id'_{IN}
-Checks if $|t_C - t_N| < \Delta t$
-Checks if
$m_2 \oplus (K_{HN} \| t_N) \overset{?}{=} (K_N \| (0)^{32}) \oplus (t_N \| (m_1 \oplus a_N))$
*Search and Find valid pair (K_N, a_N) from the $T(K_{Ni}, a_{Ni})$ for equalization, else reject.
-Generates t_H
-Picks a random r_H
-Computes $m_3 = a_N \oplus r_H$, $r_N = m_1 \oplus a_N$,
$m_4 = K_{HN} \oplus K_N \oplus h(a_N \| r_N \| r_H)$
- $K_S = h(m_1 \| r_N \| a_N \| r_H \| t_N \| m_4 \| t_H)$
- Finally, Stores session key K_S.
Authentication Phase
$\langle m_3, m_4, t_H, id'_{IN} \rangle$
$\langle m_3, m_4, t_H \rangle$
-Checks $|t'_C - t_H| < \Delta t$
-Computes $r_H = m_3 \oplus a_N$
-Checks if
$m_4 \oplus id_N \oplus b_N \overset{?}{=} h(a_N \| r_N \| r_H)$
$K_S = h(m_1 \| r_N \| a_N \| r_H \| t_N \| m_4 \| t_H)$
Finally, Stores session key K_S.

FIGURE 3. Authentication and key-agreement phase of the proposed scheme.

B. EAVESDROPPING ATTACK

In the authentication phase, the adversary can listen to and store all transmitted data, however, according to the anonymity feature, they cannot use transmitted messages to obtain a_N and K_N values of the SN to compute K_S.

C. IMPERSONATION, REPLAY AND MAN IN THE MIDDLE ATTACKS

Here, the adversary follows two goals: (1) deceiving the parties by impersonating a legal partner and (2) selecting the best strategy to correctly take a wild guess at session key identifying against a bit string equal to the key length. Therefore, due to using a timestamp, if a temporal inconsistency is detected (i.e. $|t_C - t_N > \Delta t$ or $|t'_C - t_H| > \Delta t$), the message will be rejected. In addition, the fresh random values of r_N and r_H do not reveal any modifications in the transmitted message, hence, the adversary needs to be able to change the parameters of transmitted messages to spoof messages. However, for this purpose, the adversary needs to know id_N, a_N, and b_N, a task which is impossible via eavesdropping unless the adversary captures the SN. Nevertheless, compromising the K_{HN} is not possible and it is assumed completely beyond the reach of the adversary according to the Dolev-Yao threat model. On the other hand, it will be protected by the random temporary value of K_N in Eq. (2).

D. SENSOR NODE CAPTURE ATTACK AND INTRUDING TO THE IN

Suppose the attacker can physically capture the sensor node. In this case, it should be noted whether other sensor nodes in relationship with the hub node will be compromised as a result of the forgery and disclosure of the captured sensor node or not. Hence, disclosure or forging of the sensor node tuple $< id_N, b_N, a_N >$ will not provide any important information to the adversary. Owing to calling $a_N = h(id_N \parallel K_N)$, the adversary is not aware of the secret K_N and this secret value is protected by the one-way hash function.

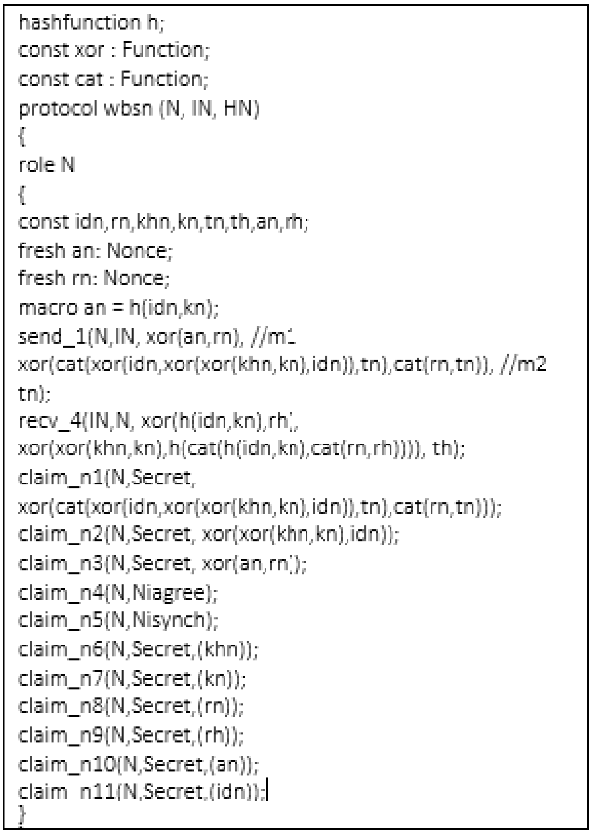
On the other hand, by recalling $b_N \oplus id_N = K_{HN} \oplus K_N$, the adversary has no information about secret values of K_{HN} and K_N, so the other sensor nodes will no longer be affected by this attack. Although the adversary is capable of stealing the *IN* (e.g. the smartphone) and penetrating it, they cannot impersonate the secure communication between the SN and HN. This is because there is no required long-term parameter stored in *IN* memory for the adversary's calculations and the only parameter stored in its memory is the 16-bits ID, which is used only for authentication by the HN and *IN* itself.

E. JAMMING AND DE-SYNCHRONIZATION

An authentication scheme is susceptible to a desynchronization attack if it requires the two parties to update their status in synchronism. Therefore, although an authentication attempt by an adversary is blocked, the SN can still retry authentication requests using the previous K_N and a_N. Since HN stores a list of (K_{Ni}, a_{Ni}) values (i represents the sensor node number) in the memory, it can constantly keep up and synchronize itself with the repeated SN requests.

F. FORWARD AND BACKWARD SECRECY

This security feature indicates that if the session key is revealed, the previous and next session keys are not exposed.



```
hashfunction h;
const xor : Function;
const cat : Function;
protocol wbsn (N, IN, HN)
{
role N
{
const idn,rn,khn,kn,tn,th,an,rh;
fresh an: Nonce;
fresh rn: Nonce;
macro an = h(idn,kn);
send_1(N,IN, xor(an,rn), //m1
xor(cat(xor(idn,xor(xor(khn,kn),idn)),tn),cat(rn,tn)), //m2
tn);
recv_4(IN,N, xor(h(idn,kn),rh),
xor(xor(khn,kn),h(cat(h(idn,kn),cat(rn,rh)))), th);
claim_n1(N,Secret,
xor(cat(xor(idn,xor(xor(khn,kn),idn)),tn),cat(rn,tn)));
claim_n2(N,Secret, xor(xor(khn,kn),idn));
claim_n3(N,Secret, xor(an,rn));
claim_n4(N,Niagree);
claim_n5(N,Nisynch);
claim_n6(N,Secret,(khn));
claim_n7(N,Secret,(kn));
claim_n8(N,Secret,(rn));
claim_n9(N,Secret,(rh));
claim_n10(N,Secret,(an));
claim_n11(N,Secret,(idn));
}
```

FIGURE 4. The SPDL code of the proposed scheme (1).

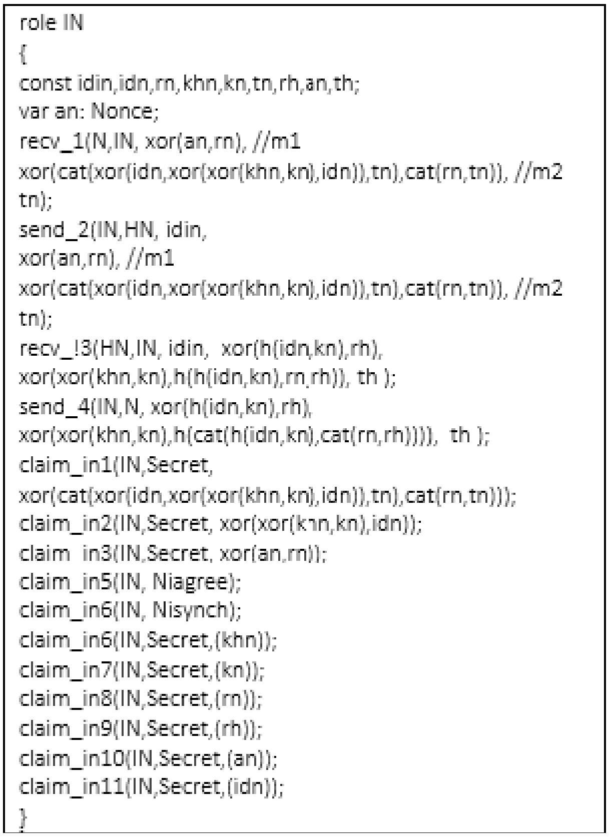
While session keys can be obtained by capturing a node, Eq. (10) and (14) are protected by a one-way hash function as well as random, fresh, and dynamic temporary parameters from the same session.

VI. FORMAL VERIFICATION VIA SCYTHER

This section uses the Scyther tool [28], [36], [37] according to the formal proof to verify the security of the proposed scheme. This tool uses the Dolev-Yao threat model as well as modifying encrypted schemes and is designed to forge information, automate authentication, and analyze the properties of security protocols [32]. The Scyther tool is developed by Python and uses the security protocol description language (SPDL). The written language can be modeled by the command line interface (CLI) and display a window using the security verification outputs against different attacks. Further, if an attack is detected, it can use the graphical user interface (GUI) to illustrate a graphical view of the detected attack [32]. Since this tool can be applied to test the claims that are defined by the tool itself, the written codes following the security verification of the authentication phase of the proposed scheme are presented at the end of this paper (Figures 4 to 7).

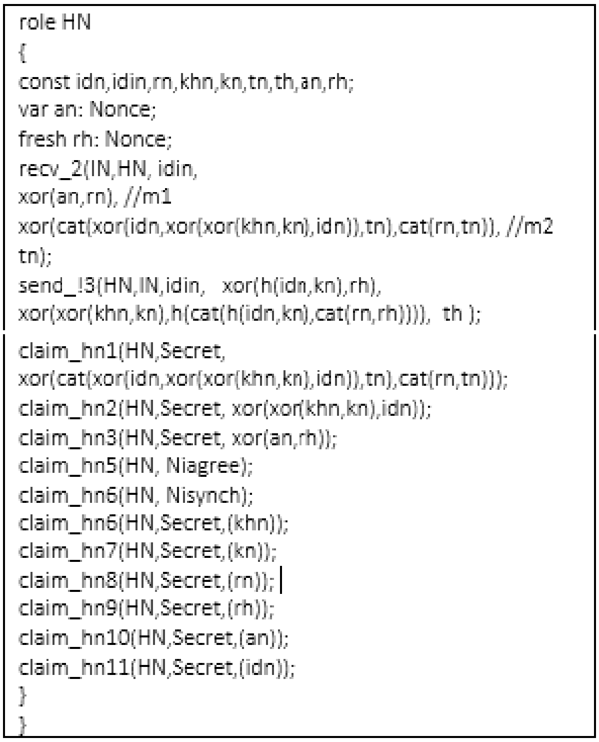
VII. EFFICIENCY ANALYSIS

This section checks and calculates the storage space, computational costs, and energy consumption of the SN and HN



```
role IN
{
const idin,idn,rn,khn,kn,tn,rh,an,th;
var an: Nonce;
recv_1(N,IN, xor(an,rn), //m1
xor(cat(xor(idn,xor(xor(khn,kn),idn)),tn),cat(rn,tn)), //m2
tn);
send_2(IN,HN, idin,
xor(an,rn), //m1
xor(cat(xor(idn,xor(xor(khn,kn),idn)),tn),cat(rn,tn)), //m2
tn);
recv_!3(HN,IN, idin,  xor(h(idn,kn),rh),
xor(xor(khn,kn),h(h(idn,kn),rn,rh)), th );
send_4(IN,N, xor(h(idn,kn),rh),
xor(xor(khn,kn),h(cat(h(idn,kn),cat(rn,rh)))),  th );
claim_in1(IN,Secret,
xor(cat(xor(idn,xor(xor(khn,kn),idn)),tn),cat(rn,tn)));
claim_in2(IN,Secret, xor(xor(khn,kn),idn));
claim  in3(IN,Secret, xor(an,rn));
claim_in5(IN, Niagree);
claim_in6(IN, Nisynch);
claim_in6(IN,Secret,(khn));
claim_in7(IN,Secret,(kn));
claim_in8(IN,Secret,(rn));
claim_in9(IN,Secret,(rh));
claim_in10(IN,Secret,(an));
claim_in11(IN,Secret,(idn));
}
```

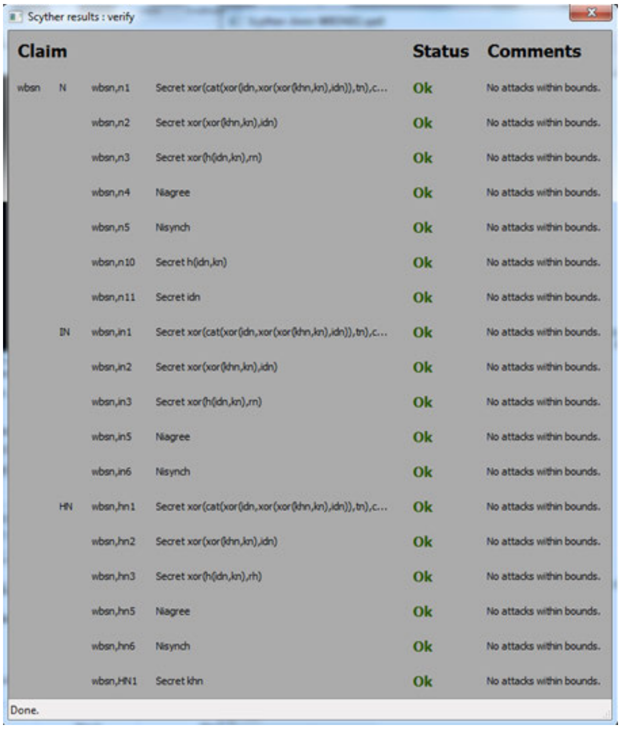
FIGURE 5. **Continue. The SPDL code of the proposed scheme (2).**



```
role HN
{
const idn,idin,rn,khn,kn,tn,th,an,rh;
var an: Nonce;
fresh rh: Nonce;
recv_2(IN,HN, idin,
xor(an,rn), //m1
xor(cat(xor(idn,xor(xor(khn,kn),idn)),tn),cat(rn,tn)), //m2
tn);
send_!3(HN,IN,idin,   xor(h(idn,kn),rh),
xor(xor(khn,kn),h(cat(h(idn,kn),cat(rn,rh)))),  th );
claim_hn1(HN,Secret,
xor(cat(xor(idn,xor(xor(khn,kn),idn)),tn),cat(rn,tn)));
claim_hn2(HN,Secret, xor(xor(khn,kn),idn));
claim_hn3(HN,Secret, xor(an,rh));
claim_hn5(HN, Niagree);
claim_hn6(HN, Nisynch);
claim_hn6(HN,Secret,(khn));
claim_hn7(HN,Secret,(kn));
claim_hn8(HN,Secret,(rn));|
claim_hn9(HN,Secret,(rh));
claim_hn10(HN,Secret,(an));
claim_hn11(HN,Secret,(idn));
}
}
```

FIGURE 6. **Continue. The SPDL code of the proposed scheme (3).**

on the same simulated device. Also, the communication cost (required bandwidth) is evaluated by the length of transmitted messages. Finally, the efficiency of the proposed scheme is compared with a number of previously proposed schemes.



Claim				Status	Comments
wbsn	N	wbsn,n1	Secret xor(cat(xor(idn,xor(xor(khn,kn),idn)),tn),c...	Ok	No attacks within bounds.
		wbsn,n2	Secret xor(xor(khn,kn),idn)	Ok	No attacks within bounds.
		wbsn,n3	Secret xor(h(idn,kn),rn)	Ok	No attacks within bounds.
		wbsn,n4	Niagree	Ok	No attacks within bounds.
		wbsn,n5	Nisynch	Ok	No attacks within bounds.
		wbsn,n10	Secret h(idn,kn)	Ok	No attacks within bounds.
		wbsn,n11	Secret idn	Ok	No attacks within bounds.
	IN	wbsn,in1	Secret xor(cat(xor(idn,xor(xor(khn,kn),idn)),tn),c...	Ok	No attacks within bounds.
		wbsn,in2	Secret xor(xor(khn,kn),idn)	Ok	No attacks within bounds.
		wbsn,in3	Secret xor(h(idn,kn),rn)	Ok	No attacks within bounds.
		wbsn,in5	Niagree	Ok	No attacks within bounds.
		wbsn,in6	Nisynch	Ok	No attacks within bounds.
	HN	wbsn,hn1	Secret xor(cat(xor(idn,xor(xor(khn,kn),idn)),tn),c...	Ok	No attacks within bounds.
		wbsn,hn2	Secret xor(xor(khn,kn),idn)	Ok	No attacks within bounds.
		wbsn,hn3	Secret xor(h(idn,kn),rh)	Ok	No attacks within bounds.
		wbsn,hn5	Niagree	Ok	No attacks within bounds.
		wbsn,hn6	Nisynch	Ok	No attacks within bounds.
		wbsn,HN1	Secret khn	Ok	No attacks within bounds.

Done.

FIGURE 7. **Security verification of the proposed scheme obtained by Scyther.**

A. STORAGE REQUIREMENT

According to Li *et al.* (Section III), $|id'_{IN}|$ is 16 bits and $|t_N| = |t_H| = 32$ bits. Since the hash function uses the SHA-1 algorithm, and the output $|a_N|$ is 160 bits, the other parameters including $|id_N|$, $|b_N|$, $|r_N|$, $|r_H|$, $|K_N|$, $|K_{HN}|$, and $|K_s|$ are also assumed to be 160 bits. Therefore, the storage space required by the $SN(|id_N, a_N, b_N, K_s)$ is 640 bits while the HN storage ($|K_{Si}$ and $|id'_{IN}, K_{HN}, T(K_{Ni}, a_{Ni})|$) is $480n + 16m + 160$ bits, where m is the number of INs and n is the number of SNs (see Table 3).

B. COMPUTATIONAL TIME AND COST

Assume t_{xor} denotes the computational time of XOR operation and t_h as the computational time for the 160-bit hash function. Note that, t_{xor} is extremely small, compared to t_h, and thus we can assume $t_{xor} \approx 0$. Accordingly, in the proposed protocol, the computational costs for the SN and HN are obtained by Eq. (15) and (16). To measure the computation time of cryptographic primitives in a hardware simulated environment, a 32-bit Cortex-M3 microcontroller with a memory of 512 KB and a frequency of 72 MHz was utilized [38]. Recalling a SHA-1 hash function also takes 0.06 ms [38]. Collectively, the computation time for two hash functions using SHA-1 is given by Eq. (17) (see Figure 8 and Table 3).

$$2t_h + 6t_{xor} \tag{15}$$

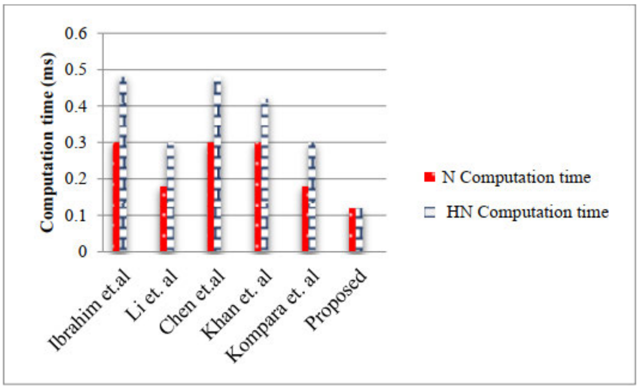


FIGURE 8. Computation time.

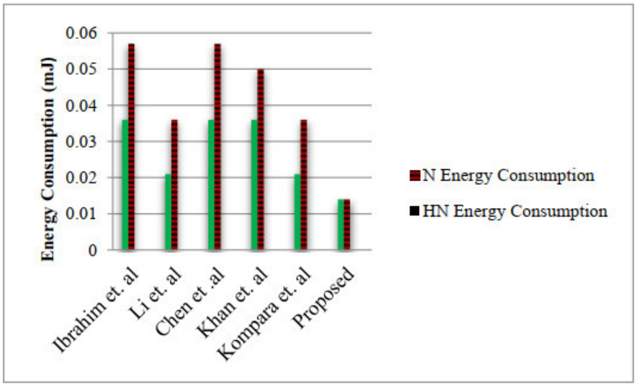


FIGURE 9. Energy consumption.

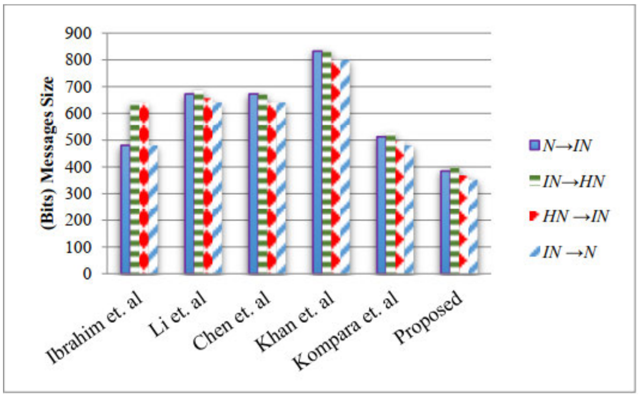


FIGURE 10. Communication cost.

$$2t_h + (2n+5)t_{xor} \tag{16}$$

$$T_{2th} = 2 \times 0.06 = 0.12ms \tag{17}$$

TABLE 2. Bandwidth used (communicant cost) per message (bit).

Steps	Ibrahim [9]	Li [15]	Chen [31]	Khan [32]	Kompara [33]	**our scheme**
$SN \to L$	480	672	672	832	512	384
$IN \to HN$	640	688	672	832	528	400
$HN \to IN$	640	656	640	800	496	368
$IN \to SN$	480	640	640	800	480	352

TABLE 3. Comparing the efficiency features running on simulated micro-controller 32-bits cortex-m3 at 72MHz.

Schemes	Node	Storage cost	Cost (cycle)
Ibrahim [9]	SN	480 bits	$5t_h + 2t_{xor} \approx 5t_h$
	HN	480n+160	$8t_h + 4t_{xor} \approx 8t_h$
Li [15]	SN	640	$3t_h + 7t_{xor} \approx 3t_h$
	HN	160(n+1)+16m	$5t_h + 12t_{xor} \approx 5t_h$
Chen [30]	SN	800	$5t_h + 5t_{xor} \approx 5t_h$
	HN	160(n+1)	$8t_h + 11t_{xor} \approx 8t_h$
Khan [31]	SN	640	$5t_h + 9t_{xor} \approx 5t_h$
	HN	160(n+1)	$7t_h + 14t_{xor} \approx 7t_h$
Kompara [32]	SN	640	$3t_h + 6t_{xor} \approx 3t_h$
	HN	640n+16m+160	$5t_h + (n+7)t_{xor} \approx 5t_h$
our scheme	SN	640	$2t_h + 6t_{xor} \approx 2t_h$
	HN	480n+16m+160	$2t_h + (2n+5)t_{xor} \approx 2t_h$

TABLE 4. Comparing the efficiency features running on simulated micro-controller 32-bits cortex-m3 at 72MHz (Continue of Table 3).

Schemes	Node	Time (ms)	Energy(mJ)
Ibrahim [9]	SN	0.30	0.036
	HN	0.48	0.057
Li [15]	SN	0.18	0.021
	HN	0.3	0.036
Chen [30]	SN	0.3	0.036
	HN	0.48	0.057
Khan [31]	SN	0.3	0.036
	HN	0.42	0.05
Kompara [32]	SN	0.18	0.021
	HN	0.3	0.036
our scheme	SN	0.12	0.014
	HN	0.12	0.014

C. ENERGY CONSUMPTION

The consumed current by the microcontroller in Section VII at room temperature (300K or 27°C) and in an active mode with a rated voltage of 3.3 V is 36 mA [27]. Therefore, the power consumed in the active state was equal to 118.8 mW, which shows a very low power consumption. Hence, according to Section VII, it is possible to use the power consumption during approximation computations. Accordingly, the energy used by either the HN or SN with two hash functions are given by Eq. (18), (see Figure 9 and table 4).

$$E_N = E_{HN} = (0.12 \times 118.8)/1000 = 0.014mJ \tag{18}$$

D. COMMUNICATION COSTS

As indicated by the authentication steps, when $SN \to IN :< m_1, m_2, t_N >$, the message is 384 bits whereas when $IN \to HN :< m_1, m_2, t_N, id'_{IN} >$, the message is 400 bits. In the return path, when $HN \to IN :< m_3, m_4, t_H, id'_{IN} >$ the message is 368 bits and in the last transmission, $IN \to SN :< m_3, m_4, t_H >$ the message is 352 bits. These outputs imply that, compared to its previous counterparts, our proposed scheme uses less bandwidth, as shown in Figure 10 and Table 2.

VIII. CONCLUSION

In the current research, a lightweight mutual authentication key-agreement protocol was proposed for a two-tier WBSN in the centralized mode. Since body sensors are highly energy-constrained, here we showed that the balance between security and performance could be maintained, while at the same time taking into account the passive mode of sensor nodes as an inherent feature. Accordingly, in each session, the previous auxiliary parameters were refreshed before the first authentication request by the SN and consequently, there was no need to update predefined parameters. As a result, the auxiliary equations and hash functions were applied less than the protocols presented in Table 3, while a proper balance between performance and security was retained too.

Concerning security, while maintaining the two criteria of anonymity and unlinkability between sessions, we investigated common vulnerabilities using the Scyther security verification tool. In this analysis, our proposed protocol exhibited desirable security. On the other hand, compared to other schemes, the SN and HN respectively consumed 53 and 70 percent less energy while also reducing the computation time by 52 and 70 percent, respectively. Furthermore, compared to previous schemes, the proposed scheme could decrease communication costs by 41 percent.

REFERENCES

[1] X. Huang, Q. Wang, C. Bangdao, A. Markham, R. Jäntti, and A. W. Roscoe, "Body sensor network key distribution using human interactive channels," in *Proc. 4th Int. Symp. Appl. Sci. Biomed. Commun. Technol. (ISABEL)*, 2011, pp. 1–5.

[2] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wireless Netw.*, vol. 17, no. 1, pp. 1–18, Jan. 2011.

[3] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. Kwak, "A comprehensive survey of wireless body area networks," *J. Med. Syst.*, vol. 36, no. 3, pp. 1065–1094, 2012.

[4] Z. R. Alashhab, M. Anbar, M. M. Singh, Y.-B. Leau, Z. A. Al-Sai, and S. A. Alhayja'a, "Impact of coronavirus pandemic crisis on technologies and cloud computing applications," *J. Electron. Sci. Technol.*, Nov. 2020, Art. no. 100059, doi: 10.1016/j.jnlest.2020.100059.

[5] T. Hayajneh, G. Almashaqbeh, S. Ullah, and A. V. Vasilakos, "A survey of wireless technologies coexistence in WBAN: Analysis and open research issues," *Wireless Netw.*, vol. 20, no. 8, pp. 2165–2199, Nov. 2014.

[6] A. Astrin, *IEEE Standard for Local and Metropolitan Area Networks—Part 15.6: Wireless Body Area Networks*, Standard 802.15.6, 2012.

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

[8] M. Toorani, "'Security analysis of the IEEE 802.15. 6 standard,'" *Int. J. Commun. Syst.*, vol. 29, no. 17, pp. 2471–2489, 2016.

[9] 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, Oct. 2016.

[10] J.-M. Ho, "A versatile suite of strong authenticated key agreement protocols for body area networks," in *Proc. 8th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2012, pp. 683–688.

[11] J. Iqbal, N. ul Amin, and A. I. Umar, "Secure anonymous mutual authentication for star two-tier wireless body area networks," in *Proc. 2nd Nat. Conf. Inf. Assurance (NCIA)*, 2013, pp. 37–50.

[12] J. Shen, H. Tan, S. Moh, I. Chung, Q. Liu, and X. Sun, "Enhanced secure sensor association and key management in wireless body area networks," *J. Commun. Netw.*, vol. 17, no. 5, pp. 453–462, Oct. 2015.

[13] K.-H. Yeh, "A secure IoT-based healthcare system with body sensor networks," *IEEE Access*, vol. 4, pp. 10288–10299, 2016.

[14] A. A. A. EL-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, and W. Mazurczyk, "Efficient quantum-based security protocols for information sharing and data protection in 5G networks," *Future Gener. Comput. Syst.*, vol. 100, pp. 893–906, Nov. 2019.

[15] C.-M. Chen, B. Xiang, T.-Y. Wu, and K.-H. Wang, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Comput. Netw.*, vol. 129, pp. 429–443, Dec. 2017.

[16] A. A. A. El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, H. Elwahsh, M. J. Piran, A. K. Bashir, O.-Y. Song, and W. Mazurczyk, "Providing end-to-end security using quantum walks in IoT networks," *IEEE Access*, vol. 8, pp. 92687–92696, 2020.

[17] W.-Z. Zhang, I. A. Elgendy, M. Hammad, A. M. Iliyasu, X. Du, M. Guizani, and A. A. A. El-Latif, "Secure and optimized load balancing for multitier IoT and edge-cloud computing systems," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 8119–8132, May 2021.

[18] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5G Internet of Things scenario," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 1, pp. 118–131, Mar. 2020.

[19] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Informat. J.*, vol. 18, no. 2, pp. 113–122, 2017.

[20] M. Salayma, A. Al-Dubai, I. Romdhani, and Y. Nasser, "Wireless body area network (WBAN): A survey on reliability, fault tolerance, and technologies coexistence," *ACM Comput. Surv.*, vol. 50, no. 1, pp. 1–38, Apr. 2017.

[21] W. Li, L. Liao, D. Gu, C. Ge, Z. Gao, Z. Zhou, Z. Guo, Y. Liu, and Z. Liu, "Security analysis of the PHOTON lightweight cryptosystem in the wireless body area network," *KSII Trans. Internet Inf. Syst.*, vol. 12, no. 1, pp. 1–21, 2018.

[22] R. A. Khan and A. S. K. Pathan, "The state-of-the-art wireless body area sensor networks: A survey," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 4, 2018, Art. no. 15501477.

[23] V. Kumar, S. Jangirala, and M. Ahmad, "An efficient mutual authentication framework for healthcare system in cloud computing," *J. Med. Syst.*, vol. 42, no. 8, pp. 1–25, Aug. 2018.

[24] R. Ali and A. K. Pal, "Cryptanalysis and biometric-based enhancement of a remote user authentication scheme for E-healthcare system," *Arabian J. Sci. Eng.*, vol. 43, no. 12, pp. 7837–7852, 2018.

[25] M. Kompara, S. Kumari, and M. Hölbl, "Analysis and improvement of a secure key management protocol for e-health applications," *Comput. Electr. Eng.*, vol. 73, pp. 97–113, Jan. 2019.

[26] 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.

[27] *Device Overview*, document STM32F103, 2016

[28] M. Tanveer, A. H. Zahid, M. Ahmad, A. Baz, and H. Alhakami, "LAKE-IoD: Lightweight authenticated key exchange protocol for the Internet of drone environment," *IEEE Access*, vol. 8, pp. 155645–155659, 2020.

[29] M. Tanveer, G. Abbas, and Z. H. Abbas, "LAS-6LE: A lightweight authentication scheme for 6LoWPAN environments," in *Proc. 14th Int. Conf. Open Source Syst. Technol. (ICOSST)*, Dec. 2020, pp. 1–6.

[30] C. M. Chen, B. Xiang, T. Y. Wu, and K. H. Wang, "An anonymous mutual authenticated key agreement scheme for wearable sensors in wireless body area networks," *Appl. Sci.*, vol. 8, no. 7, pp. 429–443, 2018.

[31] H. Khan, B. Dowling, and K. M. Martin, "Highly efficient privacy-preserving key agreement for wireless body area networks," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./ 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 1064–1069.

[32] 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.

[33] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. M. Leung, "Body area networks: A survey," *Mobile Netw. Appl.*, vol. 16, no. 2, pp. 171–193, 2011.

[34] R. Negra, I. Jemili, and A. Belghith, "Wireless body area networks: Applications and technologies," *Procedia Comput. Sci.*, vol. 83, pp. 1274–1281, Jan. 2016.

[35] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

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

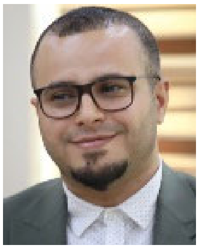
[37] L. Viganò, "Automated security protocol analysis with the AVISPA tool," *Electron. Notes Theor. Comput. Sci.*, vol. 155, pp. 61–86, May 2006.

[38] J. Liu, Q. Li, R. Yan, and R. Sun, "Efficient authenticated key exchange protocols for wireless body area networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, no. 1, p. 188, Dec. 2015.

BEHROOZ KHADEM received the B.Sc. degree in applied mathematics from the University of Tehran, Tehran, Iran, in 1991, the M.Sc. degree in applied mathematics from the Shahid Bahonar University of Kerman, Kerman, Iran, in 1995, and the Ph.D. degree in chaos-based cryptography from the Department of Mathematics, Kharazmi University, Tehran, in 2015. Since 2011, he has been a Research Assistant at the Institute of Mathematics, Kharazmi University. He has published over 50 research articles in reputed peer-reviewed journals and conference proceedings of IEEE/Springer/Elsevier. His research interests include data security and cryptography, but are not limited to applied mathematics, algorithms and complexity, computer security, chaos-based cryptography, applied cryptanalysis, security of communication networks, artificial intelligence and machine learning for security, image processing, and optimization techniques. He has served as a reviewer and a technical program committee member of multiple journals and conferences.

AMIN MASOUMI SUTEH received the B.Sc. degree in power engineering from the Mazandaran University of Science and Technology (MUST), Babol, Iran, in 2015, and the M.Sc. degree in electrical engineering-telecommunication (cryptography and secure communication) from Imam Hossein University (IHU), Tehran, Iran, in 2018. He was the Secretary of the Iranian Academic Society of Cryptology, Students' Branch, IHU, in 2017. His research interests include security protocols and provable security models.

MUSHEER AHMAD received the B.Tech. and M.Tech. degrees from the Department of Computer Engineering, Aligarh Muslim University, India, in 2004 and 2008, respectively, and the Ph.D. degree in chaos-based cryptography from the Department of Computer Engineering, Jamia Millia Islamia, New Delhi, India. From 2007 to 2010, he has worked with the Department of Computer Engineering, Aligarh Muslim University. Since 2011, he has been working as an Assistant Professor with the Department of Computer Engineering, Jamia Millia Islamia. He has published over 85 research articles in international reputed refereed journals and conference proceedings of the IEEE/Springer/Elsevier. He has more than 1400 citations of his research works with an H-index of 22. His research interests include multimedia security, chaos-based cryptography, cryptanalysis, machine learning for security, image processing, and optimization techniques. He has served as a reviewer and a technical program committee member for many international conferences. He has also served as a referee for some renowned journals, such as *Signal Processing*, *Information Sciences*, the *Journal of Information Security and Applications*, IEEE Access, the IEEE Journal on Selected Areas in Communications, the IEEE Transactions on Neural Networks and Learning Systems, IEEE Transactions on NanoBioscience, *Wireless Personal Communications*, *Neural Computing and Applications*, the *International Journal of Bifurcation and Chaos*, *Optik*, *Optics and Laser Technology*, *Neurocomputing*, *IET Information Security*, *IET Image Processing*, *Security and Communication Networks*, *Complexity*, *Computers in Biology and Medicine*, *Chaos Solitons and Fractals*, *Physica A: Statistical Mechanics and its Applications*, *Signal Processing: Image Communication*, the *Journal of the Chinese Institute of Engineers*, *Computational and Applied Mathematics*, *Concurrency and Computation*, and *ETRI Journal*.



AHMED ALKHAYYAT received the B.Sc. degree in electrical engineering from Al Kufa University, Najaf, Iraq, in 2007, the M.Sc. degree from the Dehradun Institute of Technology, Dehradun, India, in 2010, and the Ph.D. degree from Cankaya University, Ankara, Turkey, in 2015. He is currently the Dean of International Relationship and the Manager of Word Ranking with the Islamic University, Najaf. To serve his community, he acted as a reviewer for several journals and conferences. He contributed in organizing several IEEE conferences, workshop, and special sessions. His research interests include the IoT in the healthcare systems, SDN, network coding, cognitive radio, efficient-energy routing algorithms and efficient-energy MAC protocol in cooperative wireless networks and wireless body area networks, and cross-layer designing for self-organized networks.

MOHAMMAD SABZINEJAD FARASH received the B.Sc. degree in electronic engineering from the Shahid Chamran College of Kerman, in 2006, the M.Sc. degree in communication engineering from Imam Hussein University, in 2009, and the Ph.D. degree in cryptographic mathematics from the Department of Mathematics and Computer Sciences, Tarbiat Moallem University, Iran, in 2013.

His research interests include security protocols and provable security models.

HANY S. KHALIFA received the joint Ph.D. degree from the Faculty of Education, Tanta University, and the Informatics Researches Institute, Scientific City for Scientific Researches and Technological Applications, Burj Al Arab, with the recommendation of exchanging the thesis with the competent authorities, in 2013.

He is currently a Lecturer at the Department of Computer Science, Misr Institute of Commerce and Computers, Mansoura, Egypt. He is the author and coauthor of several ISI journal and conference papers, including *Multimedia Tools and Applications*, *Physica A: Statistical Mechanics and its Applications*, and *Security and Communication Networks*. His research interests include artificial intelligence, cloud computing, mobile applications, image processing, and cryptosystems.