IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 8, 2020, accepted September 19, 2020, date of publication September 24, 2020,
date of current version October 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3026630

An Efficient Lightweight Key Agreement and Authentication Scheme for WBAN

ZIA UR REHMAN, SAUD ALTAF, AND SALEEM IQBAL
University Institute of Information Technology, Pir Mehr Ali Shah Arid Agriculture University, Rawalpindi 45000, Pakistan
Corresponding author: Zia Ur Rehman (ziaraja@gmail.com)

ABSTRACT Wireless Body Area Network (WBAN) is a promising field that may improve the quality of life by using it in patients' health monitoring process. However, the mobility and open access of wireless networks have resulted in several security gaps which may lead to critical health-related data compromise issues. Therefore, there existed a need to develop a mechanism to secure patient health-related data from all security impairments. Recently, a lightweight authentication scheme that depends on the assumption that the base node is reliable is proposed. Nevertheless, it does not seem feasible practically. Hence, the researchers present a lightweight cryptographic scheme based on three levels that provide anonymous key agreement and authentication for the data communicated on the wireless channel. The proposed authentication scheme shows its efficiency to protect against various known cyber-attacks especially the base station compromise attack and sensor node impersonation attack. The scheme was formally verified with BAN logic and simulated informally using the Automated Validation of Internet Security Protocol and Applications (AVISPA) tool. The proposed key agreement and authentication scheme was also compared with the results of other related researches. The simulation results and security analysis indicate that the proposed improved scheme has overcome different identified gaps in terms of storage requirements, computational, and communicational costs.

INDEX TERMS Patient health monitoring, authentication, WBAN, communication, cyber attacks.

I. INTRODUCTION

The enhancement in technology, especially the sensor network has opened the way to improve the quality of life by making remote monitoring of patients possible. The patients' conditions have now instantly been monitored with the help of this ubiquitous technology as never before. The WBANs have provided flexibility for patients to carry on their daily life activities as well as their health is being taken good care by the specialized medical practitioner [2].

The wearable or implantable devices are attached to the patient's body to monitor its bodily features like heart rate, Blood Pressure (BP), temperature, Electrocardiography (ECG), etc., and these devices are connected with wireless technologies [3]. Therefore, WBAN provides a complete monitoring mechanism for patients without hassle. Fig. 1 shows the typical architecture for WBAN that consists of acquiring data from sensors and transmitting to the medical server through a wireless channel where a specialized doctor can easily view patient data to diagnose and prescribe accordingly [4].

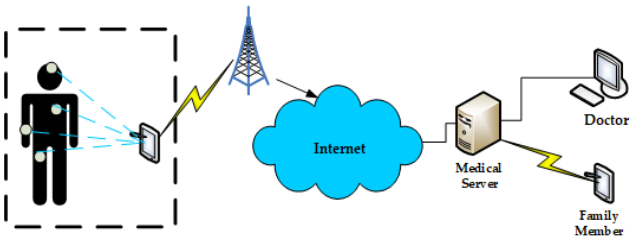

FIGURE 1. The typical architecture of WBAN.

The different types of authentication schemes have been found in the literature, a paper published by Rehman *et al.* divides the authentication schemes into four different categories namely physiological based, cryptographic based, proximity, and channel-based schemes [5]. However, other classifications are also present in the literature [6], [7]. The physiological-based schemes use the bodily features of patients for authentication [8]–[10]. These schemes are adequately appropriate in resource constraint WBAN devices.

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

However, the major drawback is their vulnerability to DoS attacks and it is difficult to measure alike physiological signals for all devices on various parts of the patient's body [11].

The cryptographic-based authentication schemes provide robust authentication with the key agreement but occupy extra storage space and are computational intensive [12]–[14]. However, Elliptic Curve Cryptography (ECC) based schemes [15], [16] have consumed less computational cost than the traditional asymmetric schemes but the lightweight schemes require even lesser computational cost as compared with the ECC schemes.

The authors of papers [17], [30] presented the authentication schemes based on channel characteristics. Such schemes are good for providing key entropy based on channel variation which results in robust authentication. The main drawback of these schemes is providing less anonymity and high computational cost [12].

Proximity-based authentication schemes [18], [19] require communicating devices apart from each other at a distance of half wavelength. This distance limitation narrows the scope of application for such schemes in WBAN and thus acts as a major drawback. Moreover, the anonymous authentication schemes in which keys are pre-deployed [20], provides high-performance efficacy and are also lightweight. These schemes use less complex mathematical operation and are very much popular in research circles for their suitability in the WBAN environment. This paper falls in the same category as well.

The schemes presented by Ibrahim *et al.* [21], Xu *et al.* [28], and Li *et al.* [12] are also lightweight, provide anonymity, based on Hash and XOR operations to ensure effectiveness. Li *et al.'s* scheme is the basis of Kompara *et al.'s* [1] work. The different authors [22], [23] have also used Li *et al.'s* scheme as a foundation for their improved version of schemes by fixing the problems in the original scheme. However, Koya *et al.* [23], proposed a hybrid scheme i.e. a blend of physiological features i.e., Electrocardiography (ECG) of a patient with the original scheme of Li *et al.* [12], and resulted in an improved scheme but exposed an additional cost of acquiring data from sensors with synchronization as well. Therefore, these related schemes [12], [21]–[23], [28] and [1] have also been selected for comparison with our scheme in section VI.

In another research, Mucchi *et al.* [31] has proposed a new modulation technique using a thermal noise loop for securing wireless communication at the physical layer level. The proposed technique has shown resilience against the DoS attack and has achieved productive advantages in a multi-user environment. Similarly, Soderi *et al.* [32] has proposed a novel physical layer watermarking based security scheme in conjunction with a jamming receiver for secure wireless communication. The results have indicated it a full-rate, energy-efficient protocol.

The major contribution of our paper is to overcome the security gaps found in Kompara *et al.* [1] by modifying their protocol to overcome the identified shortcomings as follows:-

- We have proposed an enhanced key agreement and authentication scheme based on hash and XOR functions. The proposed scheme has enhanced features like protection against Intermediate Node (IN) compromise, sensor node impersonation, and base station compromise attacks besides the security features offered by the original scheme.
- We have verified our scheme formally using BAN logic and informally using one of the renowned tool specially designed for this purpose called AVISPA.
- The proposed authentication scheme has enhanced storage and communicational costs that results in better performance when compared with peer schemes.

The rest of the paper is structured as Section 2 provides problem identification, Section 3 depicts system model and adversary model, Section 4 presents the proposed scheme, Section 5 shows the proposed scheme's security analysis i.e. security features, formal and informal analysis, Section 6 depicts the performance evaluation, and comparison of our scheme with peer work, Section 7 covers discussion on our scheme and the conclusion & future work as section 8.

II. PROBLEM IDENTIFICATION

The authentication protocol presented by Komapara *et al.* [1] provides a lightweight authentication and key establishment. The network model of their scheme consists of three-tiers as shown in the following Fig 2. In their model, tier 1 contained a sensor node denoted as N that acquires data and is resource-constrained. The Intermediary Node (IN) is usually a smartphone also called tier 2. It receives data from sensor nodes (N) and then forwards it to tier 3, the Hub node (HN). The HN is usually a medical server that is resource enriched and its job is to provide secure and efficient healthcare-related services.

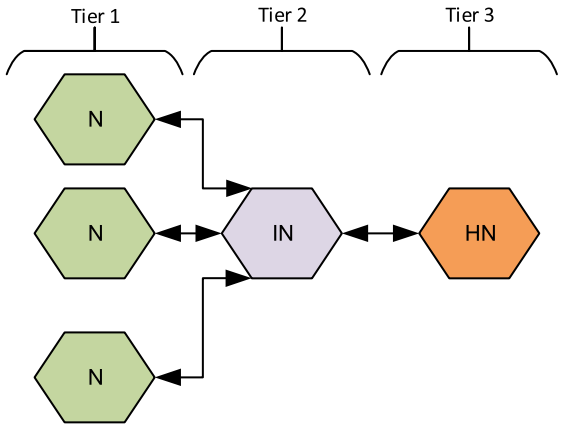

FIGURE 2. The network model of Kompara *et al.'s* scheme.

This scheme entails three parts namely initialization, registration, and authentication. Both phases i.e., initialization and registration are implemented in the role System Administrator (SA) with an assumption that the channel is secured while

the authentication phase is implemented by the role HN with an assumption of the open channel. To share secrets between N and UN, authors have assumed that the secured channel is available for SA. However, such an assumption is not held for the authentication phase, therefore, the intruder may play its part in it. The process of authentication and agreement on a common key is the responsibility of HN by establishing a communication channel secured between N and HN through a common shared key.

In the initialization phase, SA chooses the master's secret key (k_{HN}) and save it in HN's memory. While in the registration phase, SA, firstly, picks up a distinct identity (id_N) and lastly a key (k_N) for each node N. It also calculates values $x_N = h(k_{HN} \| k_N)$ and $a_N = k_{HN} \oplus k_N \oplus id_N$. SA also picks short term identity ($id_N^{'}$) in the case of the first level and saves the tuple ($id_N^{'}$, id_N,x_N, a_N) otherwise, it saves (id_N, x_N, a_N). Similarly, it stores tuple (k_{HN},k_{Nt}, id_N) in case of the second level otherwise, it saves the tuple (k_{HN},$id_N^{'}$, k_{Nt},id_N) to the memory of HN.

In the authentication phase (as shown in Fig. 3), the communication starts from N by randomly picked number r_N and current timestamp (t_N). The N then calculates, $tid_N = h(id_N \oplus t_N \| r_N)$ and sends the tuple (tid_N, a_N, b_N, t_N) to IN. The IN appends its own identity $id_{IN}^{'}$ to the received tuple and then sends it to HN. After receiving the aforesaid tuple it further checks the validity of both $id_{IN}^{'}$ and t_N otherwise, the process is aborted. It then computes $k_N \oplus id_N = k_{HN} \oplus a_N$.

The HN finds for a match of stored values of id_N,k_{Nt} *or* k_{Nr}, if not found, then the session is terminated otherwise it continues and calculates $x_N^* = h\left(k_{HN} \| k_N^*\right)$, $r_N^* = x_N^* \oplus b_N$, and $tid_N^* = h\left(id_N \oplus t_N \| r_N^*\right)$. To check the integrity of the message newly created temporary identity is matched with a previously stored one. If there is no problem then it picks k_N^+ and compute $x_N^+ = h\left(k_{HN} \| k_N^+\right), \alpha = h\left(id_N \| r_N \| x_N^+ \| x_N\right), \eta = x_N^* \oplus x_N, \mu = k_{HN} \oplus k_N^+ \oplus \alpha$ and $\beta = h\left(r_N \| x_N^+ \| \eta \| \mu\right)$. Now HN firstly sends the reply message to IN, secondly replaces k_{Nt} with k_N^+ and saves it. Lastly, it calculates the secret symmetric session key k_S=$\alpha \oplus x_N$, this key is stored on the device and is utilized for later communication. The HN composes and sends the message tuple (β, η,μ, $id_{IN}^{'}$) to IN. After receiving the tuple, IN truncates its identity $id_{IN}^{'}$ and relays the message (β, η, μ) towards N. Now, N calculates $x_N^{+*} = \eta \oplus x_N, \beta^* = h(r_N \| x_N^{+*} \| \eta \| \mu)$ and test the integrity by calculating $\beta ? = \beta^*$ which must be successful to carry forward the authentication process. It further computes $\alpha = h\left(id_N \| r_N \| x_N^+ \| x_N\right)$ and $a_N^+ = \mu \oplus \alpha \oplus id_N$. Moreover, N calculates, and session key $k_S = \alpha \oplus x_N$. Finally, it saves the session key and replaces values (x_N, a_N) with (x_N^+,a_N^+).

A. ANALYSIS OF KOMPARA'S SCHEME

After analysis of Kompara *et al.* [1] scheme in detail, three types of attacks were under investigation in their model as follows:

1) IN COMPROMISE ATTACK

Referring to Fig 2, the role of IN in the said scheme is to relay all the communication received to HN and saves tuple ($id_{IN}^{'}$). It is also noticed that neither IN is utilized to authenticate N nor IN itself is authenticated by HN. Therefore, it can turn into a vulnerability that may lead to IN compromise attack. Although the major role of IN is to perform coordination thus compromising IN would mean not only disturbing the whole coordination but leaving an opportunity for an adversary to extract identity to launch another successive attack to compromise the sensor node also. Normally IN is either smartwatch or smartphone and their risk of being stolen is also high, in such cases the probability of IN remain unintruded is very low.

2) SENSOR NODE IMPERSONATION ATTACK

If IN is compromised, which is possible, then parameters id_N and x_N can be exposed that will lead to sensor node impersonation attack, as it is also highlighted by authors of the said scheme. An adversary can become a part of the authentication process after successful capturing of the node and extracting the valid parameters as mentioned before to impersonate it with HN.

3) BASE STATION COMPROMISE ATTACK

The scheme only has an assumption that HN is secured which is infeasible in a practical sense because there is a possibility of HN being hacked. Although it is almost impossible for any adversary to generate valid tuple (β, η, μ) it can only happen by gaining access to the base station (HN). Thus compromising the HN would reveal all the secrets including the master key k_{HN}.

III. SYSTEM MODEL OF PROPOSED AUTHENTICATION SCHEME

Here we discuss the network model and rival model of our proposed scheme.

A. NETWORK MODEL

In our scheme, we have retained the network model of three-levels as proposed in [1], however, the N – IN communication is slightly different from communication between N and HN. The IN acts like a relaying node in case of N – HN communication and it is not saving any identity thus having less control over N. N – IN communication occurs when acquired data from one or more Ns is to be forwarded to HN. Thus the role of IN is supportive in whole communication which gathers data from sensor nodes and relays it towards HN. The network model is shown in Fig. 4.

B. RIVAL MODEL

We assumed an adversary can perform the subsequent activities:

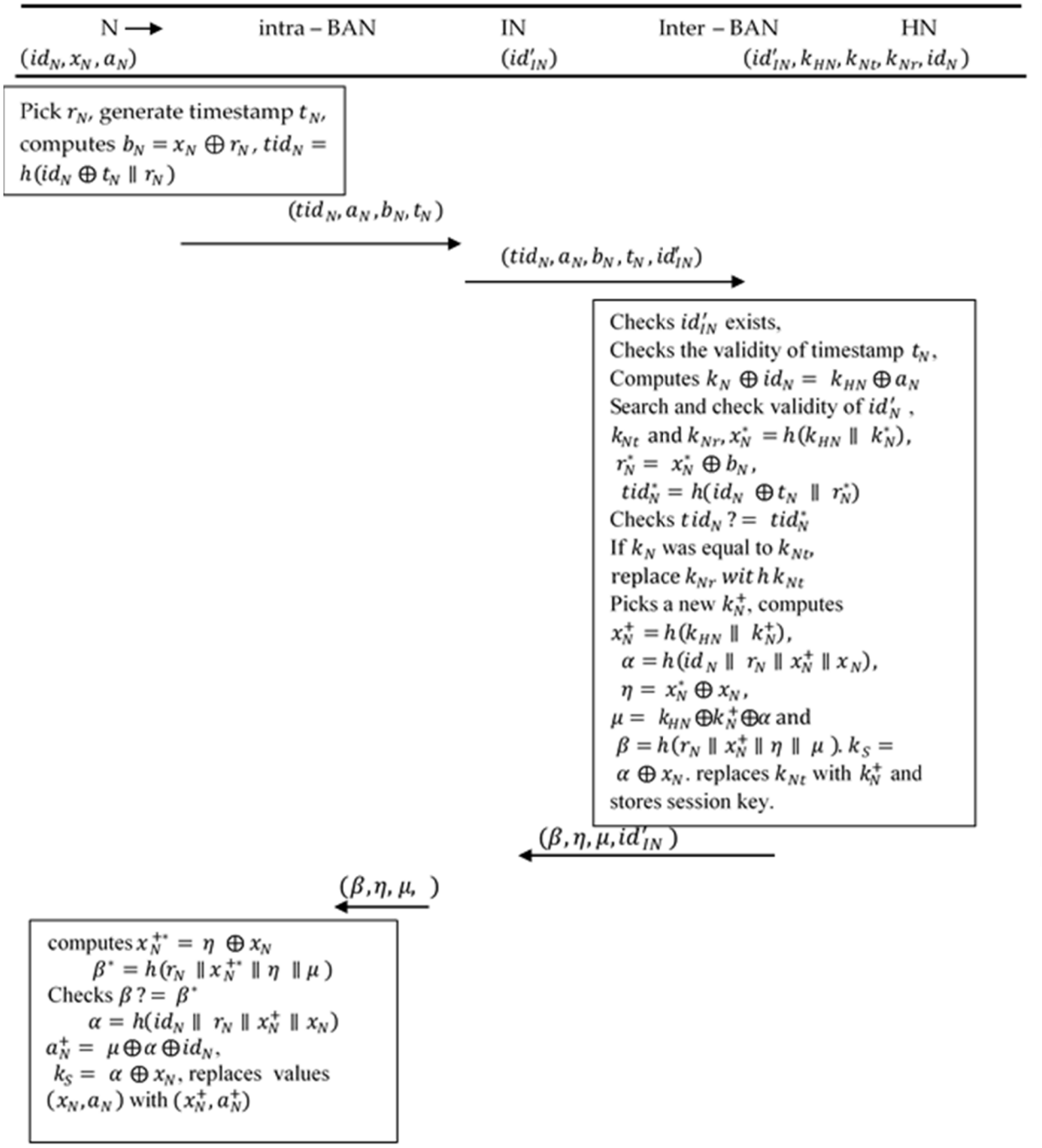

FIGURE 3. Authentication Phase of Kompara *et al.'s* scheme.

- The HN is considered as trustworthy and an adversary may not be able to retrieve the master key k_{HN}.
- The adversary may intercept the communicational channel and can falsely inject data, alter or replay older information.
- The attacker can excerpt the stored secrets by compromising the N with an intent to disrupt the mutual authentication process. Moreover, N is not protected physically due to cost factors.
- We practice well known Dolev and Yao [24] adversary model for our scheme which assumes that communicating parties use the insecure channels.

IV. PROPOSED AUTHENTICATION SCHEME

Our scheme is based on Kompara *et al.'s* [1] scheme with an intent to enhance its efficiency and to remove the security flaws present therein. Our protocol is a two-party communication protocol. We use to refer either IN or HN as

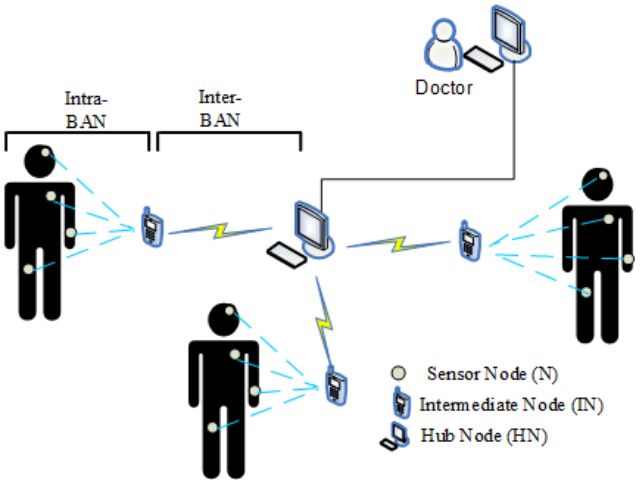

FIGURE 4. The network model of our scheme.

TABLE 1. Notation used in our scheme.

Symbol	Description
SA	System Administrator
UN	Upstream Node
N	Sensor Node
id_N	Identity of N
tid_N	Provisional ID a parameter of integrity
K_{UN}	Master key for UN
K_N	The provisional key for N
r_N	Provisional random parameter for N.
a_N, x_N, b_N, Z_N	Parameters for authentication.
α, μ, η	Parameters used for authenticating N.
β	Integrity parameter
k_S	Session key
t_N	Timestamp
h(.)	Crypto hash operation (one way)
$\|$	Concatenation operation
$\oplus$	Exclusive OR operation
x^*	Computed value without an integrity check
x^+	Net authentication round's x value.

Upstream Node (UN), the sensor node denoted as N needs to register with the UN. We have retained three phases of the original scheme and Table 1 lists the notations used.

A. INITIALIZATION PHASE

It starts with initializing UN and System Administrator (SA) do this task as:

Step 1. Picking and storing a master key K_{UN}

B. REGISTRATION PHASE

We assume N registers with either of HN or IN, both are represented as UN. The registration phase resembles Kompara *et al.'s* scheme with a few noticeable exceptions. We assumed that both initialization and registration phases are performed over secured channels. N registers as:

Step 1. A unique identity id_N is assigned.
Step 2. Key K_N is picked for N.
Step 3. $x_N = \mathrm{h}(K_{UN} || K_N)$
Step 4. $a_N = K_{UN} \oplus K_N \oplus id_N$
Step 5. $Z_N = h(K_{UN} \parallel id_N)$
Step 6. The N stores x_N, a_N, Z_N and id_N while the UN stores $K_{UN}, id_N,$ *and* K_N. The new parameter Z_N contains secret values regarding identity and key of the UN.

C. AUTHENTICATION PHASE

Unlike the other two phases, this phase is performed publicly where chances of intrusion are always present which can sabotage the whole communication. The N anonymously authenticates an upstream node (UN). This phase includes agreeing on the key and is detailed in Fig. 5.

Step 1. The N chooses a r_N and generates timestamp t_N for N and computes:
  a. $b_N = x_N \oplus r_N$,
  b. $tid_N = \mathrm{h}(id_N \oplus t_N \| r_N \| Z_N)$
  c. Sends (tid_N, a_N, b_N, t_N) to UN

Step 2. The UN checks the validity of timestamp on receiving (tid_N, a_N, b_N, t_N) and then computes:
  a. $K_N \oplus id_N = K_{UN} \oplus a_N$
  b. Find and confirm valid id_N from the stored values.
  c. $x_N^* = h(K_{UN} \parallel K_N)$, $r_N^* = x_N^* \oplus b_N$
  d. $Z_N^* = h(K_{UN} \oplus id_N)$
  e. $tid_N^* = \mathrm{h}(id_N \oplus t_N \| r_N^* \| Z_N^*)$
  f. Check $tid_N^* ? = tid_N$
  g. Pick New K_N^+, e_N
  h. $K_{UN}^+ = K_{UN} \oplus e_N$
  i. $x_N^+ = h(K_{UN}^+ \| K_N^+)$
  j. $\alpha = h\left(Z_N^* \| r_N \parallel x_N^+ \| x_N\right)$
  k. $\eta = x_N^+ \oplus Z_N^*$
  l. $\mu = K_{UN}^+ \oplus K_N^+ \oplus \alpha$
  m. $\beta = h(r_N \parallel x_N^+ \| \eta \parallel \mu)$
  n. Finally the session key
  o. $k_S = \alpha \oplus x_N^+$
  p. Now the UN sends (β, μ, η) to N.

Step 3. On receiving the tuple (β, μ, η), N will compute the following:
  a. $x_N^{+*} = \eta \oplus Z_N$
  b. $\beta^* = h(r_N \parallel x_N^{+*} \| \eta \parallel \mu)$
  c. Confirm if $\beta^* = \beta$
  d. $\alpha = h\left(Z_N^* \| r_N \parallel x_N^{+*} \| x_N\right)$
  e. $a_N^+ = \mu \oplus \alpha \oplus id_N$
  f. $k_S = \alpha \oplus x_N^{+*}$
  g. Now N replaces parameters (x_N, a_N) *with* (x_N^{+*}, a_N^+).

V. PROPOSED SCHEME'S SECURITY ANALYSIS

This section discloses three parts. Firstly, we discuss the security features provided by the proposed scheme against other cyber-attacks. Secondly, we provide security verification of

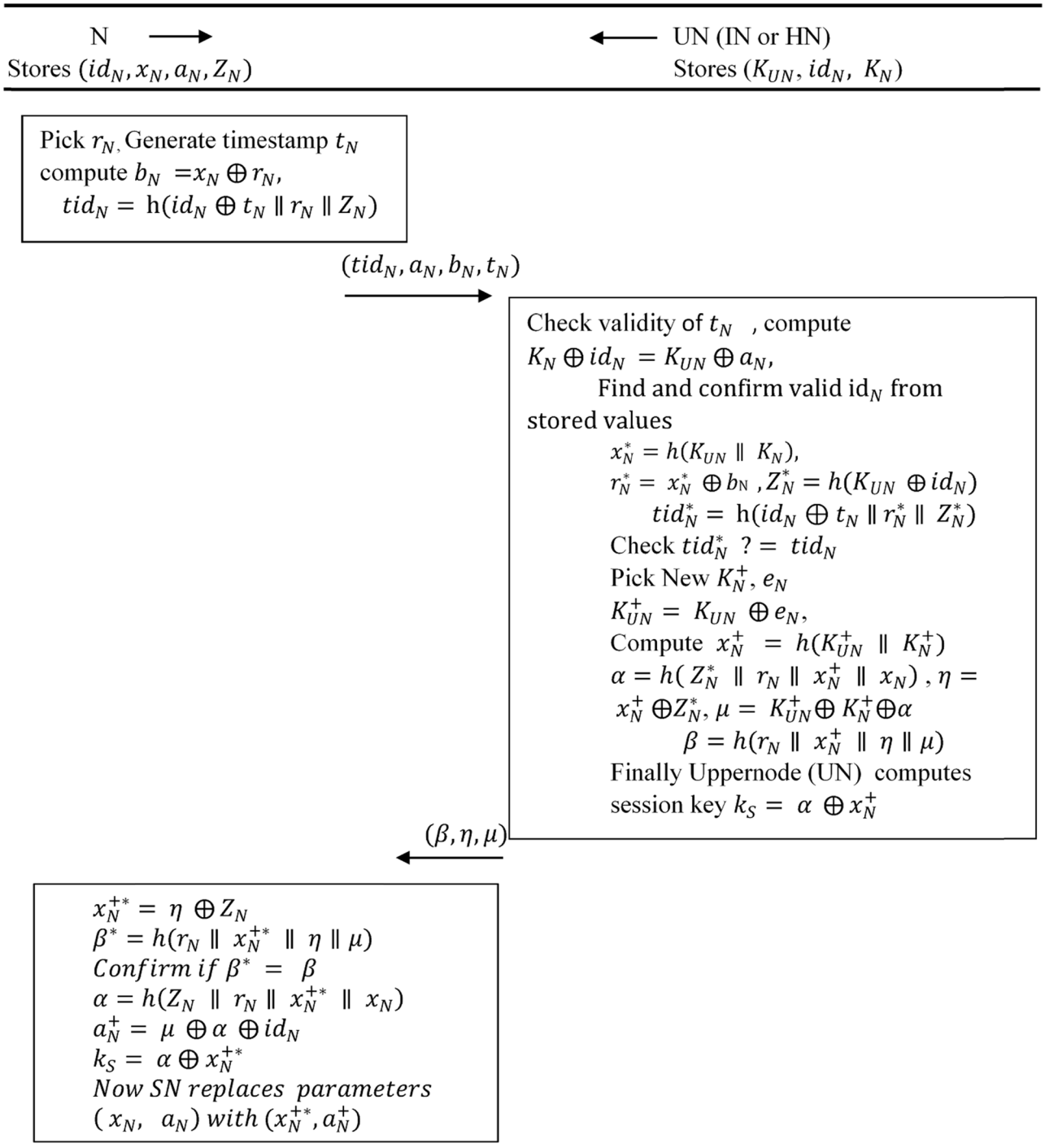

FIGURE 5. Authentication phase of proposed scheme.

the proposed scheme using BAN logic [25], and lastly, we cover informal verification using the AVISPA tool [26].

A. SECURITY FEATURES

In here, we discuss the resilience of our scheme against cyber-attacks mentioned above as well as various attacks as listed below:

1) IN COMPROMISE ATTACK

In our scheme IN no longer stores any identity, compromising it will not serve the purpose and an adversary would not be able to launch successive N impersonation attack to involve in conversation with HN. An adversary may access N in IN – N communication but nothing would be available for it to communicate with HN. It also

provides secure N – IN communication even if HN is compromised.

2) REPLAY ATTACK

It is the simplest form of attack and our scheme is protected by inserting a timestamp t_N at the start of the authentication phase. The timestamp is added in a way that the adversary cannot replace it. If a message is replayed after a while, then this change would be evident and it will be rejected. Moreover, in replaying the message a random nonce r_N is also required which changes in every request. Therefore, a replay attack is not possible

3) SENSOR NODE IMPERSONATION ATTACK

The proposed scheme provides defense against this type of attack because the adversary has no way to know the parametric values of Z_N, x_N which are required to generate a valid tuple of (tid_N, a_N, b_N, t_N) to proceed further with the authentication process.

4) HUB NODE SPOOFING ATTACK

The adversary needs to create a valid tuple i.e. (β, μ, η) because the parameter β is protected by a non-reversible hash function and the parameter η is also based on Z_N^* which can also be constructed using the hash function. Hence, this scheme provides resistance against this attack.

5) TRACKING AND ANONYMITY ATTACK

The node IN is acting as a relay that forwards messages without storing anything, therefore, a tracking attack is not possible because no information can be forged through IN. Similarly, id_N is only used to calculate tid_N which is temporary and will be changed in each session for node N to UN. Therefore, this randomly chosen parameter cannot be guessed by an adversary. So our scheme withstands against these attacks.

6) BASE STATION CAPTURE ATTACK

In our scheme, if the adversary somehow captures the HN by applying the HN stolen database attack and captures the master key K_{UN} in this case. He cannot construct the other important parameters like $x_N^+, \alpha, \beta, \eta, k_S$ because master key K_{UN} is updated by Xor operation with a new random variable e_N. The adversary has no way of knowing it because it is not publicly communicated. Therefore, our scheme also withstands against this attack.

7) FORWARD/BACKWARD SECRECY

If an adversary forges session key k_S, he could not deduce the previous session key and the subsequent session key. It is because k_S is constructed through parameters α and x_N^+ which are further based on the hash function and new fresh random value. Moreover, knowing k_S would not reveal both these parameters. Thus, this scheme holds good against this attack.

B. FORMAL PROOF USING BAN LOGIC

We use BAN logic [25] to verify that our proposed scheme provides secure key agreement and authentication between N and UN. We have to ascertain the following four goals to infer that our proposed authentication scheme is secure.

1) GOALS

G1: $UN| \equiv N| \equiv (N \overset{x_N^+}{\longleftrightarrow} UN)$
G2: $UN| \equiv (N \overset{x_N^+}{\longleftrightarrow} UN)$
G3: $N| \equiv UN| \equiv (N \overset{k_S}{\longleftrightarrow} UN)$
G4: $N| \equiv (N \overset{k_S}{\longleftrightarrow} UN)$

2) IDEALIZED FORM

The idealized form of our scheme is as under: -

Idf1: $\mathrm{N} \rightarrow UN: (N \overset{x_N^+}{\longleftrightarrow} UN, r_N, t_N)_{N \overset{id_N}{\longleftrightarrow} UN}$

Idf2: $UN \rightarrow N : (N \overset{x_N^+}{\longleftrightarrow} UN, r_N, N \overset{k_S}{\longleftrightarrow} UN)_{N \overset{id_N}{\longleftrightarrow} UN}$

3) ASSUMPTIONS

The following are the assumptions we have made to achieve the goals specified above:

A1: $UN| \equiv (N \overset{id_N}{\longleftrightarrow} UN)$
A2: $UN| \equiv \#(t_N)$
A3: $UN| \equiv N| \Longrightarrow (N \overset{x_N}{\longleftrightarrow} UN)$
A4: $N| \equiv (N \overset{id_N}{\longleftrightarrow} UN)$
A5: $N| \equiv \#(r_N)$
A6: $N| \equiv UN| \Longrightarrow (N \overset{k_S}{\longleftrightarrow} UN)$

4) FORMAL VERIFICATION (FV)

Based on the assumptions, idealized form, and inference rules, we prove the mutual key authentication feature of our proposed scheme as under: -

FV1: From Idf1, A1, and the message-meaning rule, we get

$$\frac{UN| \equiv (N \overset{id_N}{\longleftrightarrow} UN), UN \triangle \left(N \overset{x_N^+}{\longleftrightarrow} UN, r_N, t_N\right)_{N \overset{id_N}{\longleftrightarrow} UN}}{UN| \equiv N| \sim \left(N \overset{x_N^+}{\longleftrightarrow} UN, r_N, t_N\right)} \tag{1}$$

FV2: From A2 and by applying the freshness rule, we deduce:

$$\frac{UN| \equiv \#(t_N)}{UN| \equiv \#\left(N \overset{x_N^+}{\longleftrightarrow} UN, r_N, t_N\right)} \tag{2}$$

FV3: From (1), (2), and nonce verification rule, we obtain:
FV4: From (3), as shown at the bottom of the next page, and by the Believe rule, we acquire the goal G1 as:

$$\frac{UN| \equiv N| \equiv \left(N \overset{x_N^+}{\longleftrightarrow} UN, r_N, t_N\right)}{UN| \equiv N| \equiv \left(N \overset{x_N^+}{\longleftrightarrow} UN\right)} \tag{4}$$

Hence we obtain **Goal G1.**

FV5: From A3 and (4), by applying jurisdiction rule.

$$\frac{UN|\equiv N| \Longrightarrow (N \overset{x_N^+}{\longleftrightarrow} UN),\ UN|\equiv N|\equiv \left(N \overset{x_N^+}{\longleftrightarrow} UN\right)}{UN| \equiv \left(N \overset{x_N^+}{\longleftrightarrow} UN\right)} \tag{5}$$

Hence we achieve **Goal G2.**

FV6: From Idf2, A4, by applying the message meaning rule, we get

$$\frac{N|\equiv \left(N \overset{id_N}{\longleftrightarrow} UN\right),\ \triangle N(x_N, x_N^+, r_N, N \overset{k_S}{\longleftrightarrow} UN)_{N \overset{id_N}{\longleftrightarrow} UN}}{N \models UN| \sim \left(x_N, x_N^+, r_N, N \overset{k_S}{\longleftrightarrow} UN\right)} \tag{6}$$

FV7: From A5 and by applying the freshness rule, we obtain

$$\frac{N| \equiv \#(r_N)}{N| \equiv \#\left(x_N, x_N^+, r_N, N \overset{k_S}{\longleftrightarrow} UN\right)} \tag{7}$$

FV8: From (6), (7), and by nonce verification rule, we acquire

FV9: From (8), as shown at the bottom of the page, and by applying the belief rule

$$\frac{N \mid\equiv UN| \equiv \left(x_N, x_N^+, r_N, N \overset{k_S}{\longleftrightarrow} UN\right)}{N \mid\equiv UN| \equiv \left(N \overset{k_S}{\longleftrightarrow} UN\right)} \tag{9}$$

Hence we achieve **goal G3**.

FV10: From A6 and (9), by applying the jurisdiction rule (10), as shown at the bottom of the page, Hence, we obtain **goal G4**.

```
role sysadmin (
SA,HN,N          : agent,
SKs              : symmetric_key,
KUN,KN,IDN       : text,
H                : hash_func,
Snd,Rcv          : channel(dy)
)
played_by SA
def=
local State:nat,
XN,AN,ZN:text
const pidKUN,pidIDN,pidKN,hubid:protocol_id
init State:=0
transition
1. State=0/\Rcv(start) =|> State':=1/\XN':=H(KUN.KN)
/\AN':=xor(xor(KUN,KN),IDN)/\ZN':=H(IDN.KUN)
/\ Snd({IDN.XN'.AN'.ZN'}_SKs)
end role
```

FIGURE 6. The HLPSL code for SA role.

C. INFORMAL PROOF USING AVISPA

Here, we present informal verification with the help of a tool called AVISPA [26] which judges the safety of our scheme. We used a High-Level Protocol Specification Language (HLPSL) to code the protocol in the AVISPA tool. It translates HLPSL format into an Intermediate Format (IF) which is executed by backends verification models like On-the-Fly Model Check (OFMC) and Constraint Logic-based Attack Searcher (CL-AtSe). These models testify whether the scheme is safe or not and can endure against active/passive attacks [27].

The initialization, registration, and authentication phases are implemented using HLPSL roles namely: *sysadmin (SA)*, *sensornode*, and *hubnode* in HLPSL and are shown in Figures 6, 7, and 8 respectively. Furthermore, the interaction among N and HN is defined in the session role as detailed in Figure 9. The intruder knowledge, global constraints, and arrangement of one or more sessions are articulated using the environment role depicted in Figure 10. The summaries of the roles are given as under:

$$\frac{UN| \equiv \#\left(N \overset{x_N^+}{\longleftrightarrow} UN, r_N, t_N\right),\ UN \mid\equiv N| \sim \left(N \overset{x_N^+}{\longleftrightarrow} UN, r_N, t_N\right)}{UN| \equiv N| \equiv \left(N \overset{x_N^+}{\longleftrightarrow} UN, r_N, t_N\right)} \tag{3}$$

$$\frac{N| \equiv \#\left(x_N, x_N^+, r_N, N \overset{k_S}{\longleftrightarrow} UN, N \overset{id_N}{\longleftrightarrow} UN\right),\ N \mid\equiv UN| \sim \left(x_N, x_N^+, r_N, N \overset{k_S}{\longleftrightarrow} UN\right)}{N \mid\equiv UN| \equiv \left(x_N, x_N^+, r_N, N \overset{k_S}{\longleftrightarrow} UN\right)} \tag{8}$$

$$\frac{N \mid\equiv UN| \Longrightarrow (N \overset{k_S}{\longleftrightarrow} UN),\ N \mid\equiv UN| \equiv \left(x_N, x_N^+, r_N, N \overset{k_S}{\longleftrightarrow} UN\right)}{N| \equiv \left(N \overset{k_S}{\longleftrightarrow} UN\right)} \tag{10}$$

```
role sensornode (
SA,HN,N         : agent,
SKs             : symmetric_key,
H               : hash_func,
Snd,Rcv         : channel(dy)
)
played_by N
def=

local State                                             :nat,
IDN,KN,KUN,XN,AN,TN,ZN,RN,KS,KNn,ANn,XNn,Alpha,Eta,Gamma,Mu:text,
BN                                                      :message,
TIDN                                                    :hash
(text.text.text),
Beta                                                    :hash
(text.text.text.text)
const pidKUN,pidIDN,pidKN,hubid                         :protocol_id
init State:=0
transition
1. State=0 /\Rcv({IDN'.XN'.AN'.ZN'}_SKs)=|>
State':=1/\RN':=new()/\TN':=new()/\BN':=xor(XN',RN')/\TIDN':=H(xor
(IDN,TN').ZN'.RN')/\
secret(KN,pidKN,{SA,HN})/\secret(KUN,pidKUN,{SA,HN})/\secret
(IDN,pidIDN,{SA,N,HN})/\Snd({TIDN'.AN'.BN'.TN'}_SKs)

2. State=1/\Rcv(Beta'.Eta'.Mu')=|>
State':=2/\XNn':=xor(Eta',ZN)/\Beta':=H(RN.XNn'.Eta'.Mu')/\request
(N,HN,hubid,Beta)/\Alpha':=H(ZN.RN.XNn'.XN')/\ANn':=xor(xor
(Mu',Alpha'),IDN)/\KS':=xor(Alpha',XNn')/\AN':=ANn'/\XN':=XNn'/
\secret(IDN,pidIDN,{SA,N,HN})/\secret(KUN,pidKUN,{SA,HN})/\secret
(KN,pidKN,{SA,HN})
end role
```

FIGURE 7. The HLPSL code for N role.

```
role hubnode (
SA,HN,N         : agent,
KUN             : text,
SKs             : symmetric_key,
H               : hash_func,
Snd,Rcv         : channel(dy)
)
played_by HN
def=
local State                                             :nat,
IDN,KN,XN,AN,TN,ZN,RN,KS,KNn,ANn,XNn, En,Alpha,Eta,Gamma,Mu     :text,
TIDN                                                    :hash(text.text.text),
BN                                                      :message,
Beta                                                    :hash(text.text.text.text)
const pidKUN,pidIDN,pidKN,hubid                         :protocol_id
init State:=0
transition
1. State = 0/\Rcv({TIDN'.AN'.BN'.TN'}_SKs) =|>
State':= 1/\XN':= H(KUN.KNn')/\RN':=xor(XN',BN')/\ZN':=H(IDN.KUN)/\ TIDN':= H(xor
(IDN,TN').ZN'.RN')/\ KNn':= new()/\ En':=new()/\ KUN':= xor(KUN,En')/\ XNn':= H
(KUN'.KNn')/\Alpha':= H(ZN'.RN'.XNn'.XN')/\Eta':=xor(XNn',ZN')/\
Mu':=xor(xor(KUN',KNn'),Alpha')/\Beta':= H(RN'.XNn'.Eta'.Mu')/\ KS':=xor(Alpha',XNn')/
\secret(KUN,pidKUN,{SA,HN})/\secret(KN,pidKN,{SA,HN})/\secret(IDN,pidIDN,{SA,N,HN})/\
Snd({Beta'.Eta'.Mu'})/\witness(HN,N,hubid,Beta') end role
```

FIGURE 8. The HLPSL code for HN role.

```
role session(
SA,HN,N         :agent,
SKs             : symmetric_key,
%%%SK            :symmetric_key,
KUN,KN,IDN      :text,
H               :hash_func
)
def=
local SHNch,RHNch,SNch,RNch,SSAch,RSAch:channel(dy)
composition
sysadmin(SA,HN,N,SKs,KUN,KN,IDN,H,SSAch,RSAch)/\hubnode(SA,HN,N,KUN,SKs,H,SHNch,RHNch
/\sensornode(SA,HN,N,SKs,H,SNch,RNch)
end role
```

FIGURE 9. The HLPSL code for session role.

1) ROLE SYSADMIN

The SA knows all other agents, symmetric key, secret keys like KUN, KN, and identity of N i.e., IDN as shown in Figure 6. This role performs initialization and registration phases of our authentication scheme. Here, XN, AN, and ZN are declared as local variables, and their values are calculated using the Hash function. These values are then sent over a secure channel to N.

```
role environment()
def=
const sa, hn,n          :agent,
sks                     :symmetric_key,
kun,kn,idn              :text,
h                       :hash_func,
pidkun,pididn,pidkn,hubid :protocol_id
intruder_knowledge={sa,hn,n,h}
composition
session(sa,hn,n,sks,kun,kn,idn,h)
end role
goal
secrecy_of pidKUN
secrecy_of pidIDN
secrecy_of pidKN
authentication_on hubid
end goal
environment()
```

FIGURE 10. The HLPSL code for environment role.

2) ROLE SENSORNODE

This role implements the functions performed by N in the authentication phase of our scheme. Similar to the sysadmin role, sensornode (N in our scheme) knows all agents, symmetric key, send/receive channels, local variables, hash functions, and protocol_IDs. It receives the message sent by SA over the secure channel, decrypts it, and performs the functions (as depicted in Figure 7) as specified by in the proposed authentication phase over the public channel. It is also worth mentioning here that it is one of the important roles which involved actively in the authentication process.

3) ROLE HUBNODE

It is another important role played by UN and participates actively in the authentication process as detailed in Figure 8. Similar to its predecessor roles, it knows all agents, symmetric key, its secret key, local variables, hash functions protocol IDs, and send/receive channel. It receives a message from N and decrypts it using a symmetric key. It performs the rest of the functions as detailed in the authentication phase over the public channel. It then calculates the secret key at the end.

4) ROLE SESSION

In this HLPSL script as detailed in Figure 9, all agents and roles mentioned earlier are called. Moreover, initial constant parameters are declared, and send/receive channels for SA, N, HN are declared as SSAch, RSAch, SNch, RNch, SHNch, and RHNch respectively.

5) ROLE ENVIRONMENT

In here as given in Figure 10, the instances are defined for all constants. Moreover, the protocol IDs are declared, intruder knowledge is assumed and sessions are instantiated.

We have simulated our scheme using model checkers OFMC and CL-AtSe. The simulation results have shown that the scheme is safe as depicted in Figures 11 and 12 respectively.

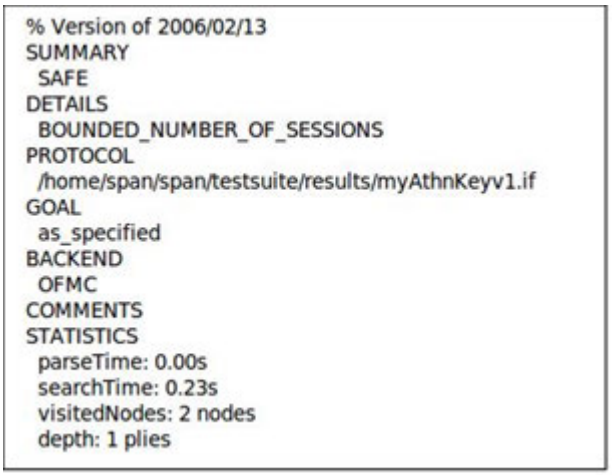

FIGURE 11. The simulation result with help of OFMC backend.

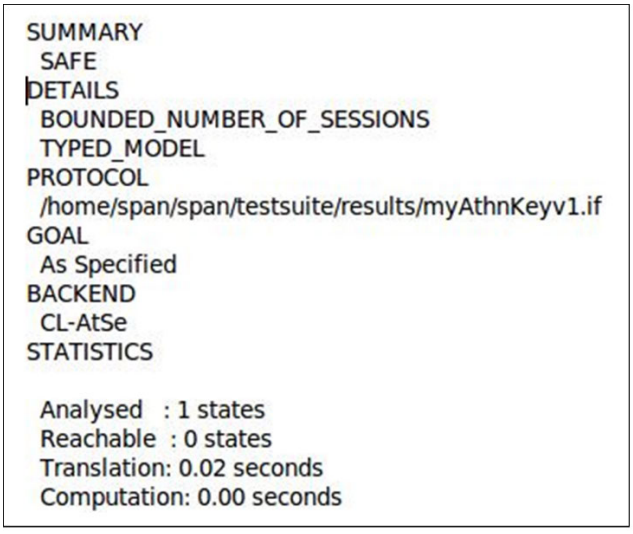

FIGURE 12. The simulation result with help of the CL-AtSe backend.

TABLE 2. Security features comparison with peer work.

	[1]	[12]	[21]	[22]	[23]	[28]	Ours
Z1	N	N	N	Y	N	N	Y
Z2	Y	Y	Y	Y	Y	Y	Y
Z3	Y	N	N	Y	Y	Y	Y
Z4	N	Y	Y	N	Y	Y	Y
Z5	Y	Y	Y	Y	Y	Y	Y
Z6	N	N	N	N	Y	N	Y
Z7	Y	Y	Y	Y	Y	Y	Y
Z8	Y	Y	Y	Y	Y	Y	Y

Z1: IN compromise attack, Z2: Replay attack, Z3, Sensor node impersonation attack, Z4: Hub node spoofing attack, Z5: Tracking and anonymity attack, Z6: Base-station capture attack, Z7: Forward/backward secrecy attack, Z8: Man-in-the-middle attack

TABLE 3. Comparison of storage cost with peer work.

Peers	N	IN	UN (HN)
[1]	640 b	16 b	(640n+16m+160) b
[12]	640 b	16 b	16m+160(n+1) b
[21]	640 b	0 b	(480n +160) b
[22]	800 b	0 b	160 b
[23]	640 b	640 b	(320+160n) b)
[28]	1280 b	32 b	(768n+32m+512) b)
Ours	800 b	0 b	(480n+160)b

n: No. of sensor nodes, m: No. of the intermediate node, b: bits

TABLE 4. Comparison of communication cost (in bits) with peer work.

Peers	N→ IN	IN→HN	HN→IN	IN→N
[1]	512	528	496	480
[12]	672	688	656	640
[21]	480	640	640	480
[22]	672	672	640	640
[23]	672	1344	960	480
[28]	832	864	1120	1088
Ours	512	512	480	480

VI. PERFORMANCE EVALUATION & COMPARISON

Here, we evaluate our scheme based on parameters like energy consumption, storage, computation, and communication cost with Kompara *et al.'s* [1] scheme as well as other peer schemes presented by Li *et al.* [12], Ibrahim *et al.* [21], Chen *et al.* [22], Koya *et al.* [23], and Xu *et al.* [28]. As explained in section I, it is worth mentioning here that we facilitate this comparison with state-of-the-art authentication scheme because they are related to each other and some of them is an improvement of earlier work. This comparison highlights the performance of the proposed authentication scheme as well. We also present a security feature comparison in Table 2 that shows our scheme fulfills all security features on which we focus on.

A. STORAGE COST

In our scheme, the N stores the tuple (id_N, x_N, a_N, Z_N), and the session key k_S. As IN in our case does not store any value, it only acts as a relay node, thus no storage is required. The UN stores parameters like K_{UN}, id_N, K_N and session key k_S 160 bits long each. Kompara *et al.'s* scheme stored 4 values on HN related to N while in our scheme only 3 values are stored on the UN. Hence our scheme is less storage-intensive in this regard. We assume that N stores parameters like $|id_N| = |x_N| = |a_N| = |Z_N| = |k_{UN}| = 160$ bits each. The storage cost is shown in Table 3 along with a comparison with peer schemes.

B. COMMUNICATION COST

In our scheme, the sensor node (N) sends the tuple (tid_N, a_N, b_N, t_N) to UN (HN) through IN which only relays it to the destination without adding anything to it. We assume $|t_N| = 32$ bits, therefore the communication cost N $\longrightarrow$ UN is $3(160) + 32 = 512$ bits and the communication cost from UN $\longrightarrow$ N is $3(160) = 480$ bits. Table 4 shows the comparison of our scheme with peers.

TABLE 5. Comparison of computational cost and time with peer work.

Peers	Node	Cost	Time
[1]	N	$3t_h + 6t_{xor} \approx 3t_h$	0.18ms
	HN	$5t_h + (n+7)t_{xor} \approx 5t_h$	0.3 ms
[12]	N	$3t_h + 7t_{xor} \approx 3t_h$	0.18ms
	HN	$5t_h + 12t_{xor} \approx 5t_h$	0.3ms
[21]	N	$5t_h + 5t_{xor} \approx 5t_h$	0.3ms
	HN	$8t_h + 4t_{xor} \approx 8t_h$	0.48ms
[22]	N	$3t_h + 5t_{xor} \approx 3t_h$	0.18ms
	HN	$5t_h + 10t_{xor} \approx 5t_h$	0.3ms
[23]	N	$5t_h + 5t_{xor} \approx 5t_h$	0.3ms
	UN	$8t_h + 11t_{xor} \approx 8t_h$	0.48ms
[28]	N	$5t_h + 5t_{xor} \approx 5t_h$	0.3ms
	HN	$7t_h + 9t_{xor} \approx 7t_h$	0.42ms
Ours	N	$3t_h + 6t_{xor} \approx 3t_h$	0.18ms
	UN	$6t_h + 10t_{xor} \approx 6t_h$	0.36ms

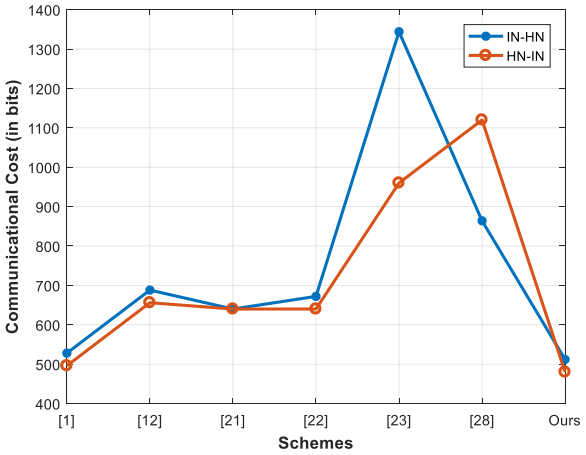

FIGURE 13. The comparison of communicational cost with peers.

TABLE 6. Comparison of energy consumption with peer work.

Peers	N (mJ)	HN (mJ)
[1]	0.021	0.036
[12]	0.021	0.036
[21]	0.036	0.057
[22]	0.021	0.036
[23]	0.036	0.048
[28]	0.036	0.0499
OURS	0.021	0.043

C. COMPUTATIONAL COST AND TIME

Let t_{xor} and t_h be the time to perform one XOR operation and one Hash function respectively. In our scheme, N performs 6 XOR operations and 3 hash functions in the authentication phase. Considering XOR operation require negligible computation so the actual computation is of the hash function, therefore, it is depicted as $3t_h + 6t_{xor} \approx 3t_h$. The total 10 XOR operations and 6 hash functions are performed in a whole scheme, so it is shown as $6t_h + 10t_{xor} \approx 6t_h$.

As the hash function in our scheme does not change (except a slight increase in the hash) so computational time cost and energy consumption are similar to Komapara's scheme. A 32-bit Cortex-M3 microcontroller at 72 MHz which is also used in Kompara *et al.* and Li *et al.*, requires 0.06 ms [29], whereas an XOR operation requires neglect-able time. Thus N requires 0.18 ms and UN requires 0.36 ms to perform a hash function. Table 5 shows a comparison of computational cost and time with peers.

D. ENERGY CONSUMPTION

The power consumption in active mode is 118.8mW which means N consumes about $0.18 * 118.8/1000 \approx 0.021$mJ and UN requires about $0.36 * 118.8/1000 \approx 0.043$mJ. Table 6 shows the comparison of energy consumption with peers.

E. COMPARISON WITH PEERS

In this section, we facilitate the comparison of our scheme with peer schemes. In our scheme, no information is stored on IN due to which the overall storage cost is less than most of the schemes compared in Table 3 except for the scheme [22] that has a similar storage cost to our scheme. Furthermore, on comparison of communication cost, it has been found that our scheme incurs comparatively low cost than the schemes shown in Table 4. It is also noticeable from Table 4 that our scheme incurs no extra cost while relaying the message through IN to UN as compared with other protocols and we have improved the communicational cost between IN – HN and vice-versa as shown in Fig. 13. Therefore, it is an efficient and lightweight scheme in this regard. It is also worth mentioning here that the communication cost for our scheme is the cost from N to UN (in our case) and vice-versa.

The computational cost and computational time for our scheme, as shown in Table 5, is also calculated and compared with other schemes. It is also evident that our scheme has a slight increase in computational cost and time as compared to Kompara *et al.* [1], Li *et al.* [12] and Koya *et al.* [23] but we comprehend it as the low price we pay for an enhanced and efficient scheme. The UN is a normally powerful device that can easily bear this burden. Moreover, Table 6 depicts the energy consumption detail of our scheme and compare it with others. It is apparent that UN (in our case) has slightly increased energy consumption but still it is lower than schemes of [21], [23], and [28].

VII. DISCUSSION

In this paper, we have proposed the new anonymous, lightweight scheme. We have analyzed the Kompara *et al.'s* [1] scheme and pointed out few security flaws. The first flaw is IN compromise attack which is caused by storing the identity id'_{IN} of IN that remain unchanged in the authentication process. The adversary can guess the identity to launch the compromise attack. Our scheme protects against this attack by not storing anything on IN and treating it as a relaying node only. The second problem is sensor node impersonation which is the aftershock of the first attack. As a solution, we calculated another secret variable

which carries the identity id_N and is protected by the non-reversible hash function. Lastly, Kompara *et al.'s* scheme is based on the assumption that HN is trustworthy and the master key k_{HN} cannot be revealed if HN is compromised. This assumption seems in-feasible practically and we have presented the solution in our scheme by updating the master key. This results in a new master key that is not available to adversary even if it compromises HN. Furthermore, we have kept the focus on keeping our scheme lightweight. The communicational cost of our scheme is comparatively lower than the peers as depicted in Fig.13. We have kept most of the computational load on HN (UN in our case) because it is normally a server and has intensive resources than N which is a resource constraint. Therefore, the computational cost and energy consumption for N is lower than the same for HN (UN in our case) as shown in Fig. 14.

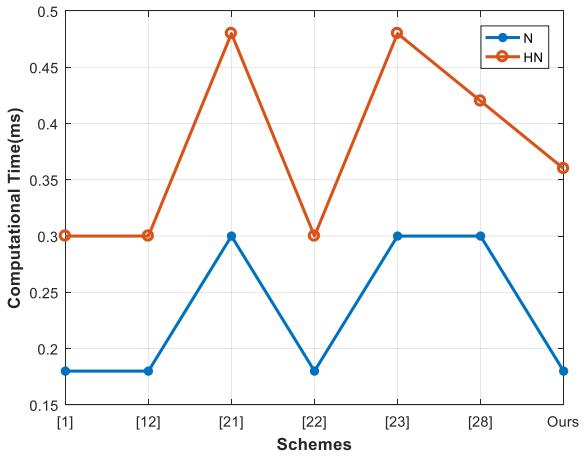

FIGURE 14. The comparison of computational cost with peers.

VIII. CONCLUSION AND FUTURE WORK

We have mainly reviewed the newly presented scheme of Kompara *et al* and highlighted the few vulnerabilities like sensor node impersonation attack, IN compromise attack, and base station capture attack. We proposed the solution to fix these vulnerabilities by preserving the anonymity and lightweight authentication scheme. Moreover, we have proved mutual authentication and key agreement of our scheme using BAN logic and we have also provided informal analysis using the AVISPA tool which proved that the new scheme withstands against well-known attacks. Furthermore, we have calculated the performance of our scheme in terms of storage, communication, computation, and energy costs. Finally, we have compared our scheme with some of the recent related work. The simulation results and security analysis has shown that proposed authentication schemes not only withstands against various known attacks but it is also an efficient, and lightweight in terms of storage, communication, computation costs, and time.

A potential future direction would be to blend this improved authentication scheme with physiological features to experience the benefits.

REFERENCES

[1] 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.
[2] C. K. Yeh, H. M. Chen, and J. W. Lo, "An authentication protocol for ubiquitous health monitoring systems," *J. Med. Biol. Eng.*, vol. 33, no. 4, pp. 415–419, 2013.
[3] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, "Wireless body area networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1658–1686, 3rd Quart., 2014.
[4] J. Wang, H. Abid, S. Lee, L. Shu, and F. Xia, "A secured health care application architecture for cyber-physical systems," *Control Eng. Appl. Informat.*, vol. 13, no. 3, pp. 101–108, 2011.
[5] Z. U. Rehman, S. Altaf, and S. Iqbal, "Survey of authentication schemes for health monitoring: A subset of cyber physical system," in *Proc. 16th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*, Jan. 2019, pp. 653–660.
[6] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustain. Cities Soc.*, vol. 50, Oct. 2019, Art. no. 101660.
[7] M. Hussain, A. Mehmood, S. Khan, M. A. Khan, and Z. Iqbal, "Authentication techniques and methodologies used in wireless body area networks," *J. Syst. Archit.*, vol. 101, Dec. 2019, Art. no. 101655.
[8] H. Tan and I. Chung, "Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor," *IEEE Access*, vol. 7, pp. 151459–151474, 2019.
[9] A. Alhayajneh, A. Baccarini, G. Weiss, T. Hayajneh, and A. Farajidavar, "Biometric authentication and verification for medical cyber physical systems," *Electronics*, vol. 7, no. 12, p. 436, Dec. 2018.
[10] P. Dodangeh and A. H. Jahangir, "A biometric security scheme for wireless body area networks," *J. Inf. Secur. Appl.*, vol. 41, pp. 62–74, Aug. 2018.
[11] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks.," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 1, pp. 8–60, 2010.
[12] 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.
[13] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2590–2601, Dec. 2017.
[14] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Gener. Comput. Syst.*, vol. 78, pp. 956–963, Jan. 2018.
[15] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Electr. Eng.*, vol. 69, pp. 534–554, Jul. 2018.
[16] 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.
[17] L. Shi, J. Yuan, S. Yu, and M. Li, "MASK-BAN: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks," *IEEE Internet Things J.*, vol. 2, no. 1, pp. 52–62, Feb. 2015.
[18] S. Mathur, R. Miller, A. Varshavsky, and W. Trappe, "ProxiMate: Proximity-based secure pairing using ambient wireless signals," in *Proc. MobiSys*, 2011, pp. 211–224.
[19] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, "Ensemble," in *Proc. 8th Int. Conf. Mob. Syst. Appl. Serv.*, vol. 10, 2010, p. 331.
[20] M. Li, S. Yu, J. D. Guttman, W. Lou, and K. Ren, "Secure ad hoc trust initialization and key management in wireless body area networks," *ACM Trans. Sensor Netw.*, vol. 9, no. 2, pp. 1–35, Mar. 2013.
[21] 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.

[22] C. Chen, B. Xiang, T. Wu, and K. Wang, "An anonymous mutual authenticated key agreement scheme for wearable sensors in wireless body area networks," *MDPI*, vol. 8, p. 1074, Dec. 2018.
[23] A. M. Koya and D. P. P., "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network," *Comput. Netw.*, vol. 140, pp. 138–151, Jul. 2018.
[24] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.
[25] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.
[26] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, and L. Compagna, "The AVISPA Tool for the Automated Validation," *Comput. Aided Verif.*, vol. 3576, pp. 281–285, 2005.
[27] D. Basin, S. Mödersheim, and L. Viganá, "OFMC: A symbolic model checker for security protocols," *Int. J. Inf. Secur.*, vol. 4, no. 3, pp. 181–208, Jun. 2005.
[28] 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.
[29] 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, pp. 1–11, Dec. 2015.
[30] M. Umar, Z. Wu, X. Liao, "Mutual authentication in body area networks using signal propagation characteristics," *IEEE Access*, vol. 8, pp. 66411–66422, 2020, doi: 10.1109/ACCESS.2020.2985261.
[31] L. Mucchi, L.S. Ronga, L. Cipriani, "A new modulation for intrinsically secure radio channel in wireless systems," *Wireless Pers. Commun.*, vol. 51, pp. 67–80, May 2009, doi: 10.1007/s11277-008-9609-8.
[32] S. Soderi, L. Mucchi, M. Hämäläinen, A. Piva, J. Iinatti, "Physical layer security based on spread-spectrum watermarking and jamming receiver," *Trans. Emerg. Telecommun. Technol.*, vol. 28, pp. 1–13, May 2017, doi: 10.1002/ett.3142.

ZIA UR REHMAN received the master's degree in computer science from Muhammad Ali Jinnah University, Islamabad, Pakistan, in 2008. He is currently pursuing the Ph.D. degree with the University Institute of Information Technology (UIIT), Pir Mehr Ali Shah Arid Agriculture University (PMAS-AAR), Rawalpindi, Pakistan. His major research interests include security issues in health monitoring aspects of cyber-physical system (CPS), the Internet of Things (IoT), and wireless sensor networks.

SAUD ALTAF received the master's degree in computer science from Iqra University, Islamabad, Pakistan, in 2007, and the Ph.D. degree in computer science from the Auckland University of Technology (AUT), New Zealand, in 2015. He is currently an Assistant Professor with the University Institute of Information Technology, Pir Mehr Ali Shah Arid Agriculture University, Rawalpindi, Pakistan. He is the author of several research publications in international journals or conferences proceedings. His research interests include wireless sensor networks, biomedical signal and image processing, the security of cyber-physical system (cps), the gesture recognition, through-the-wall radar imaging and sensing, visible light communication, the Internet of Things (IoT), artificial intelligence, and data mining.

SALEEM IQBAL received the B.S. and M.S. degrees in computer science from the COMSATS Institute of Information Technology, Pakistan, and the Ph.D. degree from the Pervasive Computing Research Group Laboratory, Faculty of Computing, Universiti Teknologi Malaysia, Malaysia, in 2015. From 2003 to 2007, he was a Lecturer with the Department of Computing Science, COMSATS Institute of Information Technology. He is currently an Assistant Professor with the University Institute of Information Technology, Pir Mehr Ali Shah Arid Agriculture University, Rawalpindi. He has over four years of experience in Pakistan Federal Government for deployment of ICT projects. To his credit, there are 15 publications. His research interests include medium access control and network layer for heterogeneous wireless networks.