


Article

Privacy-Preserving Authentication Protocol for Wireless Body Area Networks in Healthcare Applications

Hyunho Ryu and Hyunsung Kim * 

School of Computer Science, Kyungil University, Gyeongsan-si 38428, Korea; ryoofamily0430@gmail.com

* Correspondence: kim@kiu.ac.kr

Abstract: Mobile healthcare service has become increasingly popular thanks to the significant advances in the wireless body area networks (WBANs). It helps medical professionals to collect patient's healthcare data remotely and provides remote medical diagnosis. Since the health data are privacy-related, they should provide services with privacy-preserving, which should consider security and privacy at the same time. Recently, some lightweight patient healthcare authentication protocols were proposed for WBANs. However, we observed that they are vulnerable to tracing attacks because the patient uses the same identifier in each session, which could leak privacy-related information on the patient. To defeat the weakness, this paper proposes a privacy-preserving authentication protocol for WBANs in healthcare service. The proposed protocol is only based on one-way hash function and with exclusive-or operation, which are lightweight operations than asymmetric cryptosystem operations. We performed two rigorous formal security proofs based on BAN logic and ProVerif tool. Furthermore, comparison results with the relevant protocols show that the proposed protocol achieves more privacy and security features than the other protocols and has suitable efficiency in computational and communicational concerns.



Citation: Ryu, H.; Kim, H. Privacy-Preserving Authentication Protocol for Wireless Body Area Networks in Healthcare Applications. *Healthcare* **2021**, *9*, 1114. <http://doi.org/10.3390/healthcare9091114>

Academic Editors: Daniele Giansanti and Tin-Chih Toly Chen

Received: 13 July 2021

Accepted: 24 August 2021

Published: 28 August 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: healthcare service; body area network; privacy; authentication; security protocol

1. Introduction

Advances in mobile networking for Internet of Things (IoT) are powering the fourth industrial revolution. It connects physical things with digital worlds and allows for better collaboration and access across network participants, application services and people [1–5]. Wireless sensor network (WSN) technology is an essential component of IoT because it consists of a collection of sensors connected wirelessly. In the diverse kinds of WSNs, wireless body area network (WBAN) is a highly suitable communication network for medical IoT devices [6–9]. Healthcare services based on WBAN could provide remote mechanisms to monitor and collect patient's health data. The distance between patients and professional doctor can affect health status [10–13]. However, locational inequality in the medical system such as lower hospital and professional doctor is a problem that exists in almost all countries [14,15]. However, the remote healthcare system can be helpful for this problem. Especially, the remote healthcare system is beneficial for chronic diseases such as diabetes, heart failure, and chronic obstructive pulmonary disease [16]. And chronic diseases are an increasingly important concern for remote healthcare systems [17]. Because the remote healthcare system can check a patient's health status anytime and anywhere. In addition, since the patient's health status is checked in real-time, it has the advantage of able to cope quickly and the doctor can early diagnosis if the patient's health status become emergency [18,19]. Additionally, remote healthcare monitoring allows people to continue to stay at home rather than in expensive healthcare facilities such as hospitals or nursing homes [20,21].

However, privacy and security play key roles in protecting these data during data collection and transmission since remote healthcare service is vulnerable to various attacks [22–29]. If any attacker successfully launches the attacks, unintended functions may

be performed via WBAN and these can cause a life threat to the patient. Therefore, it is imperative to devise authentication and key establishment protocols for securing remote healthcare applications.

There have been many authentication protocols for WBANs in healthcare applications [30–41]. Especially, the first anonymous authentication protocol based on smartcards was proposed by Zhu et al., which provides authentication with one round message communication but keeps user anonymity [30]. However, Lee et al. showed that Zhu et al.'s protocol cannot provide perfect user anonymity and backward secrecy and proposed an enhanced protocol [31]. Zhu et al.'s protocol and Lee et al.'s protocol were based on hash operations, a symmetric key cryptography and exclusive-or operations. Memon et al. proposed an anonymous authentication protocol for location-based services, which is based on elliptic curve cryptography (ECC) [32]. Soon after Reddy et al. showed vulnerabilities of Memon et al.'s protocol focused on key compromised impersonation attack, insider attack and insecure password changing phase and a problem of imperfect mutual authentication. Reddy et al. also proposed a two-factor authentication protocol based on ECC and smartcards [33]. Memon et al.'s protocol and Reddy et al.'s protocol are depending on asymmetric key cryptography, especially ECC. For the telecare medicine information system, Khatoon et al. and Ostad-Sharif et al. separately proposed authentication and key agreement protocol based on ECC [34,35]. By adopting a fuzzy extractor for the identification of patients using biometrics, Khatoon et al.'s protocol purposed to provide secure and privacy-preserving of the patient, bilinear pairing-based, unlinkable, mutual authentication and key agreement [34]. Ostad-Sharif et al. designed an anonymous and unlinkable authentication and key agreement protocol to provide perfect forward secrecy, which provided the formal security analysis using simulation tool AVISPA result [35]. Apart from the research efforts, Ali et al. proposed an authentication and access control protocol for securing wireless healthcare WSNs [36]. Ali et al.'s protocol is based on ECC and bilinear pairing and is proven to be secure based on AVISPA tool and Burrows–Abadi–Needham (BAN) logic [37].

Primitives based on ECC or bilinear pairing have computational overhead than any other cryptographic primitives and thereby they are heavily weighted on WBANs. To cope with the overhead, Khan et al. proposed an anonymous biometric-based authentication protocol using chaotic maps [38]. To use biometrics in the protocol, Khan et al. hired the Chebyshev chaotic map and hash function, which is a lightweight authentication cryptographic primitives. Aman et al. proposed a lightweight authentication protocol over WBANs, which are based on physical unclonable functions (PUFs) [39]. Aman et al.'s protocol is based on hash functions and exclusive-or operations. Even if two protocols from Khan et al. and Aman et al. provide operational efficiency, PUF assumption is a big burden to WBANs environment. Xu et al. proposed a lightweight anonymous authentication and key agreement protocol for WBANs without using the chaotic map nor PUFs [40]. Their protocol is only based on a hash function and exclusive-or operations and has an advantage in operational cost. However, Alzahrani et al. showed that Xu et al.'s protocol is vulnerable against replay attacks and key compromise impersonation attacks and suffers from the offline identity-guessing attack [41]. Furthermore, they proposed an improved protocol for WBANs in healthcare applications. Even though Alzahrani et al.'s protocol provides a lightweight computational overhead with various advantages on security and privacy concerns, we found that Alzahrani et al.'s protocol does not provide unlinkability of patients because it uses the same identifier of access point in each session.

The contributions of this paper are as follows:

- (1) A new privacy-preserving authentication protocol for WBANs in remote healthcare applications is devised. In the protocol, an entity could protect privacy and security with a session key establishment for secure communication.
- (2) The proposed protocol utilizes lightweight operations, which are based on the hash function and exclusive-or operation. This makes the protocol suitable for WBANs in remote healthcare applications.

(3) The formal security proof in BAN logic [37] demonstrates that the proposed protocol supports privacy and security. The formal security verification with ProVerif tool [42] shows that the proposed protocol can withstand both passive and active attacks. The informal analysis of its privacy and security is presented to verify the robustness of the proposed protocol against the well-known attacks.

(4) Efficiency analysis is done based on the complexity analysis of computation and communication overheads. The results show that the proposed protocol has a little overhead than the existing protocols.

The remainder of this paper is structured as follows. Section 2 summarizes the preliminaries of the research focused on healthcare system configuration, CK threat model and design goals. Section 3 gives a detailed description of the proposed privacy-preserving authentication protocol for remote healthcare applications. Section 4 demonstrates the formal, semi-formal and informal privacy and security results of the proposed protocol. Section 5 shows performance results focused on computation and communication. Section 6 provides discussion of importance of this research with future works. Section 7 concludes the work.

2. Preliminaries

In the digital age, hospitals and health service providers have pursued innovations for rich healthcare services. WBAN technology allows patients to be treated always even in remote areas and enables doctors to diagnose diseases and treat patients in medical institutions. And its technology can help anyone to easily access medical information [43]. It also serves to reduce patient anxiety by providing easy access to current medical information such as coronavirus disease 2019 (COVID-19). This section briefly reviews a system configuration for the target remote healthcare service and the design goals of the proposed protocol.

2.1. System Configuration

The target remote healthcare service is based on WBAN for patients. As shown in Figure 1, there are three main entities, which are a patient (PT) with some sensor nodes (SNs) on WBAN, access point (AP) and hub node (HN) as a server of the remote healthcare system. Especially, a system administrator (SA) is required for the system set-up but HN could do this role instead if it is necessary. The roles of each entity are defined as follows:

- SA: It sets up system parameters and registers participants by deploying important secret values in the memory of each party.
- HN: It has a very important role as the central server for the healthcare service, which collects and keeps a database of electronic health records (EHRs) for the registered PTs. In addition to this, it works also as a registration center for all network participants and issues SNs and APs for PTs. Furthermore, it works as an authentication server to check the authenticity of system entities.
- AP: AP works as a communication gateway from SN to HN and vice versa via wireless communication link. Thereby, it does not perform any validation of messages. It is assumed that an AP belongs to a specific PT only.
- SN: Some SNs are deployed on a PT, as notated as 1, 2, 3, 4 and 5 in the left part of Figure 1, to form a WBAN by HN or SA, which do the role of collecting EHR data of the PT and transmitting them to HN. An SN has sensors to check the purposed health status such as body temperature, blood pressure, electrocardiogram and so on. It needs to consider EHR privacy because the healthcare service is data sensitive.
- PT: PT is a subject of the remote healthcare service. Normally, PT does not take part in the network communication directly but subscribes the service to SA or HN. Then, SA or HN issues some SNs and an AP of the PT for the service.
- Doctor: Doctors make the diagnosis based on PT's EHRs by accessing HN. Doctors need to regularly check the health status of PTs and provide proper medical treatments via on-line.

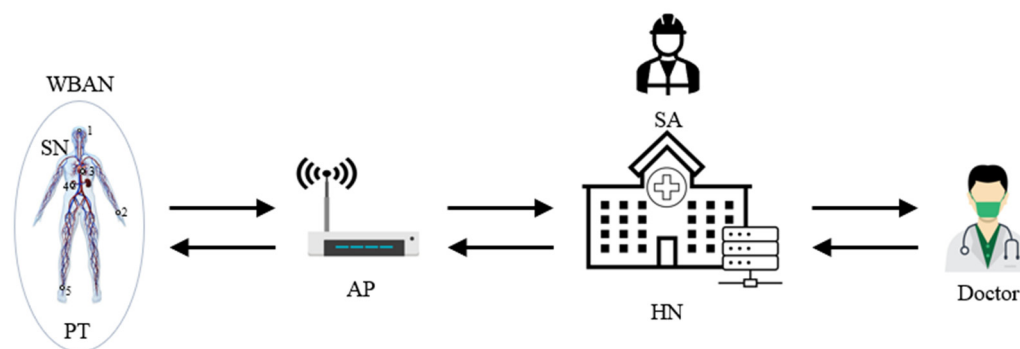


Figure 1. System configuration for remote healthcare service.

2.2. CK Threat Model

This subsection describes the widely accepted and well-known Canetti and Krawczyk (CK) threat model, which defines the ability of an adversary and is one of the foundations for formal privacy and security analysis on cryptographic protocol [44,45]. In the CK model, the adversary can fully control the communication links by listening to, altering, deciding on and injecting into the transferring information. Apart from these basic adversarial capabilities, in this model, it is assumed that the adversary can obtain secret information stored in the parties' memories via explicit attacks. As a result, the security of an authentication protocol should guarantee that the leakage of private values, such as session ephemeral secrets, would have the least possible influence on the security of other sessions and other private credentials of the communicating entities.

2.3. Design Goals

The healthcare system should provide privacy and security at the same time [46,47]. Normally, only anonymity is considered to provide privacy of PT in some other protocols in [40,41]. However, we also need to further consider unlinkability as another important privacy feature. To design a new authentication protocol for the remote healthcare service based on the CK threat model, the following five security properties and two privacy requirements are considered in this paper.

[SP1] Mutual authentication: To allow only authorized PT to get the medical services provided by HN, mutual authentication between SN and HN is required.

[SP2] Session key agreement: After a successful process of mutual authentication, further EHR data communications between SN and HN should be encrypted based on the session key to achieve confidentiality and integrity.

[SP3] Message freshness: Each entity in the system needs to check message freshness to cope with various attacks. It could be supported either by using timestamp or random nonce.

[SP4] Perfect forward secrecy: It could assure that the security of the system will not be compromised even if long-term secrets used in the protocol are compromised.

[SP5] Attack resistance: Due to the open environment in the remote healthcare service, the transmitted messages among network entities may be intercepted, modified and replayed by the adversary. Therefore, the proposed authentication protocol should be able to withstand various attacks, such as replay attack, impersonation attack, man-in-the-middle attack and known session-specific temporary information attack.

[PP1] Anonymity: Anonymity is an important privacy feature in the remote healthcare service. To protect the identity privacy of PT, the proposed protocol should guarantee that no one can get the PT's identity from the intercepted messages on the public channels.

[PP2] Unlinkability: Unlinkability is another important privacy feature in the remote healthcare service, which guarantees that the adversary cannot distinguish whether these different session's messages are related or not. The cryptographic protocol should not only guarantee the PT's anonymity but also provide unlinkability between sessions.

3. Proposed Authentication Protocol

In this section, a privacy-preserving authentication protocol for WBANs in healthcare service is proposed. The proposed protocol uses only the hash function with exclusive-or operations to provide the design goals. We assume that all the participants are synchronized on time using any proper scheme and a maximum transmission delay Δt is agreed on mutually. The proposed protocol consists of four phases, i.e., initialization phase, registration phase, authentication phase and identity modification phase. First of all, the initialization phase sets up a security building block for the overall network. PT possessed with SN and AP is a target for the registration phase to either SA or HN. The authentication phase is for the basic security service to check whether the entity is legal or not and is also to set up a session key for further secure communications. The identity modification phase is used when PT wants to change SN's identity for privacy reasons. Table 1 defines the symbols and their meanings used in this paper.

Table 1. Notations.

Notation	Descriptions
SA	System administrator
HN	Healthcare central server
PT	Patient
SN	Sensor node
AP	Access point
ID_{SN}	Identity of SN
ID_{AP}	Identity of AP
Y_{SN}	Pseudonym identity of SN
PID_{AP}	Pseudonym identity of AP
KS_{HN}	Long-term master key of HN
K_S	Established session key
T_{i_j}	i -th timestamp of an entity j
S_{i_j}	i -th random number of an entity j
a_{SN}, na_{SN}, q	Random numbers
HC_i	Hash chain value of SN
$h()$	Secure one-way hash function
$ $	Concatenation operation
\oplus	Exclusive-or operation
Δt	Allowed transmission delay

3.1. Initialization Phase

For the system initialization, SA performs the following steps.

Step 1. SA selects a long-term master key KS_{HN} for HN.

Step 2. SA stores KS_{HN} in the memory of HN.

3.2. Registration Phase

When a PT wants to subscribe to a remote healthcare service, HN performs the following steps after issuing SN and AP for PT as shown in Figure 2. All parameters are established by HN for WBANs over a secure channel.

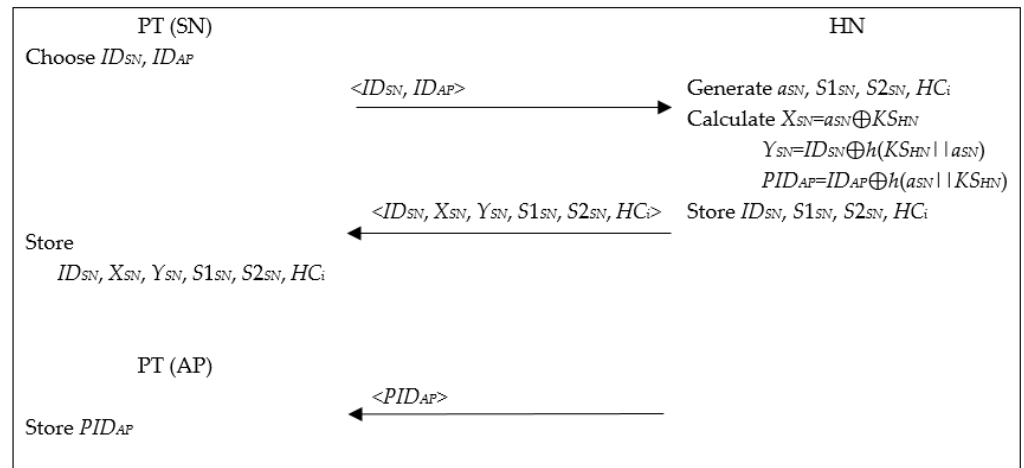


Figure 2. Registration phase.

- Step 1. PT chooses two identities ID_{SN} and ID_{AP} for SN and AP, respectively, and sends them to HN. After receiving the information, HN generates four random numbers a_{SN} , $S1_{SN}$, $S2_{SN}$ and HC_i for SN, forms a set $\langle ID_{SN}, S1_{SN}, S2_{SN}, HC_i \rangle$ and stores it in the memory.
- Step 2. After that, HN calculates $X_{SN} = a_{SN} \oplus KS_{HN}$, $Y_{SN} = ID_{SN} \oplus h(KS_{HN} || a_{SN})$ and $PID_{AP} = ID_{AP} \oplus h(a_{SN} || KS_{HN})$, composes a set $\langle ID_{SN}, X_{SN}, Y_{SN}, S1_{SN}, S2_{SN}, HC_i \rangle$ and stores it in the memory of SN. They are used for authenticity check of PT.
- Step 3. HN stores PID_{AP} in the memory of AP.

3.3. Authentication Phase

When a PT wants to use the subscribed remote healthcare service, PT with SN and AP needs to use this phase to log-in HN as shown in Figure 3. SN does whole roles of PT periodically to send the predefined sensed EHR data to HN via AP. This phase has two purposes, mutual authentication and session key agreement. Timestamp in each message is used to provide message freshness, which is used to cope with the replay attack. The detailed steps are as follows:

- Step 1. SN gets the current timestamp $T1_{SN}$, calculates a message authentication code $RID_S = (ID_{SN} || X_{SN} || Y_{SN} || S2_{SN} || HC_i || T1_{SN})$ and composes a message $\{X_{SN}, Y_{SN}, RID_S, T1_{SN}\}$ to submit to AP.
- Step 2. When AP receives the message, it adds a session dependent pseudo identity PID_{AP} to the message $\{X_{SN}, Y_{SN}, RID_S, T1_{SN}, PID_{AP}\}$ and sends the message to HN.
- Step 3. When HN receives the message, it gets the current timestamp $T1_{HN}$ and verifies the freshness of the message by validating $T1_{HN} - T1_{SN} \leq \Delta t$ where Δt is the allowed transmission delay of the network. If it does not hold, HN treats this message as a replay attack and aborts the session. Otherwise, HN calculates $a_{SN}' = X_{SN} \oplus KS_{HN}$ and $ID_{AP}' = PID_{AP} \oplus h(a_{SN}' || KS_{HN})$. After that, HN calculates $ID_{SN}' = Y_{SN} \oplus h(KS_{HN} || a_{SN}')$ and compares it with ID_{SN} stored in its memory. Only if the verification is successful, HN calculates $RID_S' = h(ID_{SN}' || X_{SN} || Y_{SN} || S2_{SN} || HC_i || T1_{SN})$ using the parameters in its repository. Finally, HN checks whether RID_S' is equal to RID_S or not.
- Step 4. Only after all verifications are successful, HN could believe the authenticity of SN and AP and forms a reply message with two options, one is to be authenticated to SN and AP and another is to update the authentication parameters for the next authentication for SN and AP, respectively. For this, HN gets the current timestamp $T2_{HN}$, generates two random numbers q and na_{SN} , and calculates $X_{SN}' = na_{SN} \oplus KS_{HN}$, $Y_{SN}' = ID_{SN}' \oplus h(KS_{HN} || na_{SN})$, $NPID_{AP} = ID_{AP}' \oplus h(na_{SN} || KS_{HN})$, $j = ID_{SN}' \oplus Y_{SN} \oplus X_{SN}$, $r = q \oplus j$, $g = h(q || j || S2_{SN})$, $Z_{AP} = h(PID_{AP} || NPID_{AP} || ID_{AP}')$,

- $NX_{SN} = X_{SN}' \oplus g$, $NY_{SN} = Y_{SN}' \oplus g$, $C_{SN} = h(q \parallel ID_{SN}' \parallel j \parallel X_{SN}' \parallel Y_{SN}' \parallel T2_{HN})$ and $K_S = h(q \parallel S1_{SN} \parallel S2_{SN} \parallel HC_i)$. After that, HN overwrites $S1_{SN}$ into $S2_{SN}$ and changes $S2_{SN}$ with K_S in its memory, which are used for the next authentication for privacy provision. And then, HN calculates $HC_i' = h(HC_i)$ and replaces it to HC_i as $HC_i = HC_i'$, which is for updating the session key parameter. After that, HN composes a message $\{r, NX_{SN}, NY_{SN}, C_{SN}, T2_{HN}, NPID_{AP}, Z_{AP}\}$ and sends it to AP.
- Step 5. After receiving the message, AP checks the freshness of message by calculating $Z_{AP}' = h(PID_{AP} \parallel NPID_{AP} \parallel ID_{AP})$ and verifying whether Z_{AP}' is the same as Z_{AP} in the message or not. Only if the verification is successful, AP overwrites $NPID_{AP}$ into PID_{AP} in its memory. After that, AP drops $NPID_{AP}$ and Z_{AP} from the message and sends the reformed message $\{r, NX_{SN}, NY_{SN}, C_{SN}, T2_{HN}\}$ to SN.
- Step 6. When SN receives the message, it gets the current timestamp $T2_{SN}$ and verifies the freshness of the message by validating $T2_{SN} - T2_{HN} \leq \Delta t$. If it is not successful, SN aborts the session, which is treated as a replay attack. Otherwise, it calculates $j' = ID_{SN} \oplus Y_{SN} \oplus X_{SN}$, $q' = r \oplus j'$, $g' = h(q \parallel j' \parallel S2_{SN})$, $X_{SN}'' = NX_{SN} \oplus g'$, $Y_{SN}'' = NY_{SN} \oplus g'$ and $C_{SN}' = h(q' \parallel ID_{SN} \parallel j' \parallel X_{SN}'' \parallel Y_{SN}'' \parallel T2_{HN})$ and validates C_{SN}' by comparing it with C_{SN} in the message. It aborts the session if the validation fails. Otherwise, SN implicitly accept the authenticity of HN and calculates a session key $K_S' = h(q' \parallel S1_{SN} \parallel S2_{SN} \parallel HC_i)$ and overwrite $S1_{SN}$ into $S2_{SN}$ and changes $S2_{SN}$ with K_S . SN replaces the two parameters, X_{SN}'' and Y_{SN}'' into X_{SN} and Y_{SN} , respectively, which are the next authentication parameters. Finally, SN calculates $HC_i' = h(HC_i)$ and replaces it to HC_i as $HC_i = HC_i'$, which is for updating the session key parameter.

3.4. Identity Modification Phase

Whenever a PT wants to change his (or her) identity, this phase should be performed. To change identity of PT, SN sends the identity modification request to HN. Then HN provides identity modification parameter only after the successful authentication. The phase is performed as follows:

- Step 1. SN sets the current timestamp $T1_{SN}$, selects a new identity ID_{SN}^{NEW} , calculates $NID_{SN} = ID_{SN}^{NEW} \oplus S2_{SN}$ and $RID_S = h(ID_{SN} \parallel X_{SN} \parallel Y_{SN} \parallel S2_{SN} \parallel NID_{SN} \parallel HC_i \parallel T1_{SN})$, composes a message $\{X_{SN}, Y_{SN}, RID_S, T1_{SN}, NID_{SN}\}$ and submits it to AP.
- Step 2. When AP receives the message, it adds PID_{AP} to the message $\{X_{SN}, Y_{SN}, RID_S, T1_{SN}, NID_{SN}, PID_{AP}\}$ and sends the message to HN.
- Step 3. When HN receives the message, it sets the current timestamp $T1_{HN}$. And HN validates the freshness of the message by verifying $T1_{HN} - T1_{SN} \leq \Delta t$. If T_{SN} is not fresh, HN aborts the session. Otherwise, HN calculates authentication parameters $a_{SN}' = X_{SN} \oplus KS_{HN}$ and $ID_{AP}' = PID_{AP} \oplus h(a_{SN}' \parallel KS_{HN})$. After that, HN calculates $ID_{SN}' = Y_{SN} \oplus h(KS_{HN} \parallel a_{SN}')$ and compares it with ID_{SN} stored in its memory. Only if the verification is successful, HN calculates $RID_S' = h(ID_{SN}' \parallel X_{SN} \parallel Y_{SN} \parallel S2_{SN} \parallel NID_{SN} \parallel HC_i \parallel T1_{SN})$ using the parameters in its repository. Finally, HN checks whether RID_S' is equal to RID_S .
- Step 4. Only after all verifications are successful, HN withdraws the new identity from SN by computing $ID_{SN}^{NEW'} = NID_{SN} \oplus S2_{SN}$. After that, HN generates current timestamp $T2_{HN}$ and random numbers q and calculates the new identity related authentication parameters $Y_{SN}' = ID_{SN}^{NEW'} \oplus h(KS_{HN} \parallel a_{SN}')$, $j = ID_{SN} \oplus Y_{SN} \oplus X_{SN}$, $r = q \oplus j$, $g = h(q \parallel j \parallel S2_{SN})$, $NY_{SN} = Y_{SN}' \oplus g$ and $C_{SN} = h(q \parallel ID_{SN} \parallel j \parallel Y_{SN}' \parallel T2_{HN})$. Then HN overwrites $ID_{SN}^{NEW'}$ into ID_{SN} in its memory. Next HN composes a message $\{r, NY_{SN}, C_{SN}, T2_{HN}\}$ and sends it to AP.
- Step 5. After receiving the message, AP sends the message $\{r, NY_{SN}, C_{SN}, T2_{HN}\}$ to SN.
- Step 6. When SN receives the message, it sets the current timestamp $T2_{SN}$. And SN validates the freshness of the message by verifying $T2_{SN} - T2_{HN} \leq \Delta t$. If $T2_{HN}$ is not fresh, SN aborts the session. Otherwise, SN calculates $j' = ID_{SN} \oplus Y_{SN} \oplus X_{SN}$, $q' = r \oplus j'$, $g' = h(q \parallel j' \parallel S2_{SN})$, $Y_{SN}'' = NY_{SN} \oplus g'$ and $C_{SN}' = h(q' \parallel ID_{SN} \parallel j' \parallel Y_{SN}'' \parallel T2_{SN})$.

$T2_{HN}$), which are withdrawing the new identity related authentication parameters. After that, SN validates C_{SN}' by comparing it with C_{SN} in the message. It aborts the session if the validation fails. Otherwise, SN replaces Y_{SN} with Y_{SN}'' in its memory.

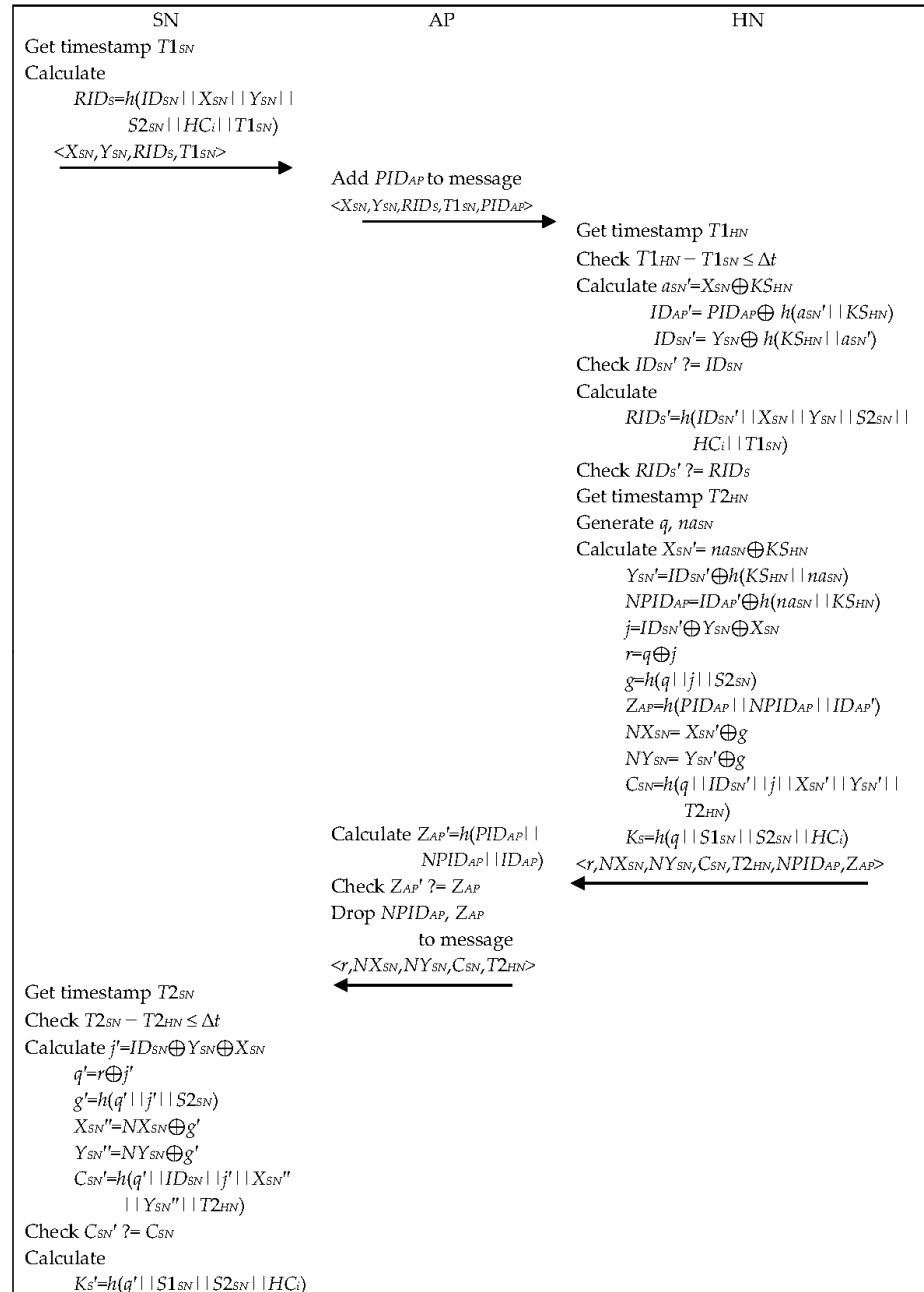


Figure 3. Authentication phase.

4. Security and Privacy Results

This section provides security analysis of the proposed protocol by using BAN logic and ProVerif tool based on the CK threat model [37,42]. Then, we demonstrate that the proposed protocol can achieve higher privacy and security features than the other related protocols.

4.1. BAN Logic Result

In this subsection, we analyze the security of the proposed protocol based on BAN logic. BAN logic is a widely adopted major formal method of valuation of any authen-

tication protocol. BAN logic analyses using axioms to verify message origin, message freshness and faithful of the origin of the message [37]. The notations in formal security analysis for BAN logic are listed as follows:

- $Q \mid \equiv X$: Principal Q believes the statement X .
- $\#(X)$: Formula X is fresh.
- $Q \mid \Longrightarrow X$: Principal Q has jurisdiction over the statement X .
- $Q \mid \triangleleft X$: Principal Q sees the statement X .
- $Q \mid \sim X$: Principal Q once said the statement X .
- (X, Y) : Formula X or Y is one part of the formula (X, Y) .
- $\langle P \rangle_Q$: Formula P combined with the formula Q .
- $Q \stackrel{SK}{\longleftrightarrow} R$: Principal Q and R may use the shared session key, SK to communicate among each other. SK is good, in that any principal except Q and R will never discover it.

In addition, we use the following BAN logic rules to prove that the proposed protocol provides a secure mutual authentication between SN, AP and HN:

- Message-meaning rule: $\frac{R \mid \equiv R \stackrel{Y}{\longleftrightarrow} S, R \triangleleft \langle X \rangle_Y}{R \mid \equiv S \mid \sim X}$
- Nonce-verification rule: $\frac{R \mid \equiv \#(X), R \mid \equiv S \mid \sim X}{R \mid \equiv S \mid \equiv X}$
- Jurisdiction rule: $\frac{R \mid \equiv S \mid \Longrightarrow X, R \mid \equiv S \mid \equiv X}{R \mid \equiv X}$
- Freshness rule: $\frac{R \mid \equiv \#(X)}{R \mid \equiv \#(X, Y)}$

To show how the proposed protocol provide secure mutual authentication between SN and HN, we need to achieve the following goals:

Goal 1: $HN \mid \equiv (HN \stackrel{K_S}{\longleftrightarrow} SN)$

Goal 2: $SN \mid \equiv (SN \stackrel{K_S}{\longleftrightarrow} HN)$

Goal 3: $HN \mid \equiv SN \mid \equiv (SN \stackrel{K_S}{\longleftrightarrow} HN)$

Goal 4: $SN \mid \equiv HN \mid \equiv (HN \stackrel{K_S}{\longleftrightarrow} SN)$

Idealized form: The arrangement of the transmitted messages between SN, AP and HN in the proposed protocol to the idealized forms is as follows:

Message 1. SN \rightarrow AP: $\langle X_{SN} \rangle_{K_{SHN}}, \langle Y_{SN} \rangle_{K_{SHN}}, \langle RIDs \rangle_{K_{SHN}}, T1_{SN}$

Message 2. AP \rightarrow HN: $\langle X_{SN} \rangle_{K_{SHN}}, \langle Y_{SN} \rangle_{K_{SHN}}, \langle RIDs \rangle_{K_{SHN}}, T1_{SN}, \langle PID_{AP} \rangle_{K_{SHN}}$

Message 3. HN \rightarrow AP: $\langle r \rangle_{K_{SHN}}, \langle NX_{SN} \rangle_{K_{SHN}}, \langle NY_{SN} \rangle_{K_{SHN}}, \langle C_{SN} \rangle_{K_{SHN}}, \langle NPID_{AP} \rangle_{K_{SHN}}, \langle Z_{AP} \rangle_{K_{SHN}}, T2_{HN}$

Message 4. AP \rightarrow SN: $\langle r \rangle_{K_{SHN}}, \langle NX_{SN} \rangle_{K_{SHN}}, \langle NY_{SN} \rangle_{K_{SHN}}, \langle C_{SN} \rangle_{K_{SHN}}, T2_{HN}$

Assumptions: The following are the initial assumptions of the proposed protocol:

A1: $HN \mid \equiv \#(T1_{SN})$

A2: $HN \mid \equiv \#(T2_{SN})$

A3: $SN \mid \equiv \#(T1_{HN})$

A4: $SN \mid \equiv \#(T2_{HN})$

A5: $SN \mid \equiv HN \stackrel{X_{SN}}{\longleftrightarrow} SN$

A6: $HN \mid \equiv HN \stackrel{X_{SN}}{\longleftrightarrow} SN$

A7: $SN \mid \equiv HN \Longrightarrow HN \stackrel{X_{SN}}{\longleftrightarrow} SN$

A8: $HN \mid \equiv SN \Longrightarrow HN \stackrel{X_{SN}}{\longleftrightarrow} SN$

Proof. In the following, we prove the test goals in order to show the secure authentication using BAN logic rules and the assumptions. \square

Based on Message 1, we could derive:

Step 1. $AP \triangleleft (\langle X_{SN} \rangle_{K_{SHN}}, \langle Y_{SN} \rangle_{K_{SHN}}, \langle RIDs \rangle_{K_{SHN}}, T1_{SN})$

Based on Step 1, AP adds $\langle PID_{AP} \rangle_{K_{SHN}}$ to the message and sends it to HN. Based on Message 2, we could derive:

Step 2. $HN \triangleleft (\langle X_{SN} \rangle_{K_{SHN}}, \langle Y_{SN} \rangle_{K_{SHN}}, \langle RIDs \rangle_{K_{SHN}}, T1_{SN}, \langle PID_{AP} \rangle_{K_{SHN}})$

According to assumption A6 and the message-meaning rule, we get:

Step 3. $HN \mid \equiv AP \mid \sim (\langle X_{SN} \rangle_{K_{SHN}}, \langle Y_{SN} \rangle_{K_{SHN}}, \langle RIDs \rangle_{K_{SHN}}, T1_{SN}, \langle PID_{AP} \rangle_{K_{SHN}})$
According to assumptions A1 and A2 and the freshness concatenation rule, we get:

Step 4. $HN \mid \equiv \# (\langle X_{SN} \rangle_{K_{SHN}}, \langle Y_{SN} \rangle_{K_{SHN}}, \langle RIDs \rangle_{K_{SHN}}, T1_{SN}, \langle PID_{AP} \rangle_{K_{SHN}})$
According to Steps 3 and 4 and the nonce verification rule, we get:

Step 5. $HN \mid \equiv SN \mid \equiv (\langle X_{SN} \rangle_{K_{SHN}}, \langle Y_{SN} \rangle_{K_{SHN}}, \langle RIDs \rangle_{K_{SHN}}, T1_{SN}, \langle PID_{AP} \rangle_{K_{SHN}})$
According to Step 5, assumption A6 and the believe rule, we get:

Step 6. $HN \mid \equiv SN \mid \equiv (HN \xrightarrow{K_{SHN}} SN)$
According to assumption A8 and the jurisdiction rule, we get:

Step 7. $HN \mid \equiv (HN \xrightarrow{K_{SHN}} SN)$
According to Steps 5, 6 and 7 and the nonce verification rule, we conclude:

Step 8. $HN \mid \equiv SN \mid \equiv (SN \xrightarrow{K_S} HN)$ (**Goal 3**)
According to assumption A8 and the jurisdiction rule, we get:

Step 9. $HN \mid \equiv (HN \xrightarrow{K_S} SN)$ (**Goal 1**)
Based on Message 3, we could derive:

Step 10. $AP \triangleleft (\langle r \rangle_{K_{SHN}}, \langle NX_{SN} \rangle_{K_{SHN}}, \langle NY_{SN} \rangle_{K_{SHN}}, \langle C_{SN} \rangle_{K_{SHN}}, \langle NPID_{AP} \rangle_{K_{SHN}}, \langle Z_{AP} \rangle_{K_{SHN}}, T2_{HN})$

According to the message meaning rule, we get:

Step 11. $AP \mid \equiv HN \mid \sim (\langle r \rangle_{K_{SHN}}, \langle NX_{SN} \rangle_{K_{SHN}}, \langle NY_{SN} \rangle_{K_{SHN}}, \langle C_{SN} \rangle_{K_{SHN}}, \langle NPID_{AP} \rangle_{K_{SHN}}, \langle Z_{AP} \rangle_{K_{SHN}}, T2_{HN})$

Based on Step 10, AP drops $\langle NPID_{AP} \rangle_{K_{SHN}}$ and $\langle Z_{AP} \rangle_{K_{SHN}}$ to the message and sends it to HN.

Based on Message 4, we derive:

Step 12. $SN \triangleleft (\langle r \rangle_{K_{SHN}}, \langle NX_{SN} \rangle_{K_{SHN}}, \langle NY_{SN} \rangle_{K_{SHN}}, \langle C_{SN} \rangle_{K_{SHN}}, T2_{HN})$
According to assumption A5 and the message-meaning rule, we get:

Step 13. $SN \mid \equiv AP \mid \sim (\langle r \rangle_{K_{SHN}}, \langle NX_{SN} \rangle_{K_{SHN}}, \langle NY_{SN} \rangle_{K_{SHN}}, \langle C_{SN} \rangle_{K_{SHN}}, T2_{HN})$
According to assumptions A3 and A4 and the freshness concatenation rule, we get:

Step 14. $SN \mid \equiv \# (\langle r \rangle_{K_{SHN}}, \langle NX_{SN} \rangle_{K_{SHN}}, \langle NY_{SN} \rangle_{K_{SHN}}, \langle C_{SN} \rangle_{K_{SHN}}, T2_{HN})$
According to Steps 12 and 13 and the nonce verification rule, we get:

Step 15. $SN \mid \equiv HN \mid \equiv (\langle r \rangle_{K_{SHN}}, \langle NX_{SN} \rangle_{K_{SHN}}, \langle NY_{SN} \rangle_{K_{SHN}}, \langle C_{SN} \rangle_{K_{SHN}}, T2_{HN})$
According to Step 14, assumption A5 and the believe rule, we get:

Step 16. $SN \mid \equiv HN \mid \equiv (HN \xrightarrow{K_{SHN}} SN)$
According to assumption A7 and the jurisdiction rule, we get:

Step 17. $SN \mid \equiv (HN \xrightarrow{K_{SHN}} SN)$
According to Steps 14, 15 and 16 and the nonce verification rule, we get:

Step 18. $SN \mid \equiv HN \mid \equiv (SN \xrightarrow{K_S} SN)$ (**Goal 4**)
According to assumption A7 and the jurisdiction rule, we get:

Step 19. $SN \mid \equiv (SN \xrightarrow{K_S} HN)$ (**Goal 2**)

According to Steps 9 and 19, the proposed authentication protocol successfully achieves the four goals. Both SN and HN could believe that they share the common session key $K_S = K'_S = h(q' \parallel S1_{SN} \parallel S2_{SN})$.

4.2. ProVerif Result

ProVerif is an automated tool for verifying security in cryptographic protocol [42]. It is supposed to be based on the CK threat model for security verification. ProVerif is a powerful tool that can verify all the possible attacks regarding mutual authentication. It also can prove safety of security properties for mutual authentication. For ProVerif analysis, we first define two channels ch1 and ch2 as public channels, among SN, AP and HN. In the ProVerif analysis, we used svalueA and svalueB to validate the session dependency. There are four events to check mutual authentication between SN and HN, which are SHbegin(entity), HSbegin(entity), SHend(entity) and HSend(entity). Session key security could be proved based on two queries, query attacker(svalueA) and query

attacker(svalueB) based on the shared session key. For the basic operations, we defined Hash(bitstring) and XOR(bitstring, bitstring) for a one-way hash function and an exclusive-or operation, respectively. After defining processes of each entity, we performed a ProVerif demo for the entities of SN, AP and HN.

We have configured the ProVerif code as follows:

```

(*-The two public channel-*)
free ch1: channel.
free ch2: channel.
(*-The basic type-*)
type entity.
type nonce.
type key.
(*-Hash operation-*)
fun Hash(bitstring): bitstring.
(*-XOR operation-*)
fun XOR(bitstring, bitstring): bitstring.
equation forall x: bitstring, y: bitstring;
XOR(XOR(x, y), y) = x.
(*-Concat operation-*)
fun Con(bitstring, bitstring): bitstring.
fun Enc(bitstring, key): bitstring.
reduc forall x: bitstring, y: key;
Dec(Enc(x, y), y) = x.
(*-Type conversion-*)
fun nontobit(nonce): bitstring [data, typeConverter].
fun bittokey(bitstring): key [data, typeConverter].
(*-The basic variables-*)
free SN, AP, HN: entity. (*-three entities in the proposed protocol-*)
free T1SN: bitstring.
free T2HN: bitstring.
free S1SN: bitstring.
free S2SN: bitstring.
free HCi: bitstring.
free KSHN: bitstring[private]. (*-public key-*)
(*-Authentication queries-*)
event SHbegin(entity).
event SHend(entity).
event HSbegin(entity).
event HSend(entity).
query t: entity; inj-event(SHend(t)) ==> inj-event(SHbegin(t)).
query t: entity; inj-event(HSend(t)) ==> inj-event(HSbegin(t)).
(*-Queries-*)
free svalueA, svalueB: bitstring [private].
query attacker(svalueA);
attacker(svalueB).
(*-SN-*)
let processSN(IDSN: bitstring, XSN: bitstring, YSN: bitstring) =
let (RIDs: bitstring) = Hash(Con(IDSN, Con(XSN, Con(YSN, Con(S2SN,
Con(HCi, T1SN)))))) in
event HSbegin(HN);
(*- SN > AP -*)
out(ch1, (XSN, YSN, RIDs, T1SN, true));
(*- AP > SN -*)
in(ch1, (r: bitstring, NXSN: bitstring, NYSN: bitstring, CSN: bitstring));

```

```

let (xj: bitstring) = XOR(IDSN, XOR(YSN, XSN)) in
let (xq: bitstring) = XOR(r, xj) in
let (xg: bitstring) = Hash(Con(xq, Con(xj, S2SN))) in
let (xXSN: bitstring) = XOR(NXSN, xg) in
let (xYSN: bitstring) = XOR(NYSN, xg) in
let (xCSN: bitstring) = Hash(Con(xq, Con(IDSN, Con(xj, Con(xXSN, Con(xYSN,
T2HN)))))) in
if xCSN = CSN then
let (xKs: bitstring) = Hash(Con(xq, Con(S1SN, Con(S2SN, HCi))) in
event SHend(SN);
out(ch1, Enc(svalueA, bittokey(xKs)).
(*-AP-*)
let processAP(IDAP: bitstring, PIDAP: bitstring) =
in(ch1, (XSN: bitstring, YSN: bitstring, RIDs: bitstring));
(*- AP > HN -*)
out(ch2, (XSN, YSN, RIDs, T1SN, PIDAP, true));
(*- HN > AP -*)
in(ch2, (r: bitstring, NXSN: bitstring, NYSN: bitstring, CSN: bitstring, NPIDAP: bit-
string, ZAP: bitstring));
let (xZAP: bitstring) = Hash(Con(PIDAP, Con(NPIDAP, IDAP))) in
if xZAP = ZAP then
(*- AP > SN -*)
out(ch1, (r, NXSN, NYSN, CSN, T2HN, true)).
(*-HN-*)
let processHN(IDAP: bitstring, IDSN: bitstring) =
in(ch2, (XSN: bitstring, YSN: bitstring, RIDs: bitstring, PIDAP: bitstring));
let (a: bitstring) = XOR(XSN, KSHN) in
let (xIDAP: bitstring) = XOR(PIDAP, Hash(Con(a, KSHN))) in
let (xIDSN: bitstring) = XOR(YSN, Hash(Con(KSHN, a))) in
if xIDSN = IDSN then
let (xRIDs: bitstring) = Hash(Con(IDSN, Con(XSN, Con(YSN, Con(S2SN, Con(HCi,
T1SN)))))) in
if xRIDs = RIDs then
event SHbegin(SN);
new q: nonce;
new nasn: nonce;
let (xXSN: bitstring) = XOR(nontobit(nasn), KSHN) in
let (xYSN: bitstring) = XOR(IDSN, Hash(Con(KSHN, nontobit(nasn)))) in
let (NPIDAP: bitstring) = XOR(IDAP, Hash(Con(nontobit(nasn), KSHN))) in
let (j: bitstring) = XOR(IDSN, XOR(YSN, XSN)) in
let (r: bitstring) = XOR(nontobit(q), j) in
let (g: bitstring) = Hash(Con(nontobit(q), Con(j, S2SN))) in
let (ZAP: bitstring) = Hash(Con(PIDAP, Con(NPIDAP, IDAP))) in
let (NXSN: bitstring) = XOR(xXSN, g) in
let (NYSN: bitstring) = XOR(xYSN, g) in
let (CSN: bitstring) = Hash(Con(nontobit(q), Con(IDSN, Con(j, Con(xXSN, Con(xYSN,
T2HN)))))) in
let (Ks: bitstring) = Hash(Con(nontobit(q), Con(S1SN, Con(S2SN, HCi))) in
(*- HN > AP -*)
out(ch2, (r, NXSN, NYSN, CSN, T2HN, NPIDAP, ZAP, true));
event HSend(HN);
out(ch2, Enc(svalueB, bittokey(Ks))).
(*-Start process-*)
process(

```

```

new XSN: bitstring;
new YSN: bitstring;
new PIDAP: bitstring;
new IDSN: bitstring;
new IDAP: bitstring;
(!processSN(IDSN, XSN, YSN)) |
(!processAP(IDAP, PIDAP)) |
(!processHN(IDAP, IDSN))
)

```

Figure 4 shows ProVerif result, which provides the successful security validation of the proposed protocol. From the result, we could find that “Query inj-event(SHend(t)) ==> inj-event(SHbegin(t)) is true.” and “Query inj-event(HSend(t)) ==> inj-event(HSbegin(t)) is true.” Those are to show mutual authentication property and replay attack resistance of the proposed protocol. After “Query not attacker (svalueA[]) is true.” and “Query not attacker (svalueB[]) is true.” show the anonymity of network participants and secrecy of the shared session key. It shows that the proposed protocol is properly performed by the tool without having any problems. As a result, we could conclude that the proposed protocol could establish a secure session key between SN and HN and the CK adversary could not discover the session key.

ProVerif text output:

```

Completing equations...
Completing equations...
-- Process 1-- Query inj-event(SHend(t)) ==> inj-event(SHbegin(t)) in process 1
Translating the process into Horn clauses...
Completing...
200 rules inserted. Base: 200 rules (32 with conclusion selected). Queue: 28 rules.
400 rules inserted. Base: 365 rules (32 with conclusion selected). Queue: 10 rules.
Starting query inj-event(SHend(t)) ==> inj-event(SHbegin(t))
RESULT inj-event(SHend(t)) ==> inj-event(SHbegin(t)) is true.
-- Query inj-event(HSend(t)) ==> inj-event(HSbegin(t)) in process 1
Translating the process into Horn clauses...
Completing...
200 rules inserted. Base: 200 rules (32 with conclusion selected). Queue: 24 rules.
Starting query inj-event(HSend(t)) ==> inj-event(HSbegin(t))
RESULT inj-event(HSend(t)) ==> inj-event(HSbegin(t)) is true.
-- Query not attacker(svalueA[]): not attacker(svalueB[]) in process 1
Translating the process into Horn clauses...
Completing...
200 rules inserted. Base: 198 rules (32 with conclusion selected). Queue: 20 rules.
Starting query not attacker(svalueA[])
RESULT not attacker(svalueA[]) is true.
Starting query not attacker(svalueB[])
RESULT not attacker(svalueB[]) is true.

-----
Verification summary:

Query inj-event(SHend(t)) ==> inj-event(SHbegin(t)) is true.

Query inj-event(HSend(t)) ==> inj-event(HSbegin(t)) is true.

Query not attacker(svalueA[]) is true.

Query not attacker(svalueB[]) is true.

-----

```

Figure 4. ProVerif result.

4.3. Informal Privacy and Security Analysis

As mentioned in [48], past research over the last thirty decades has told us that, a security proof is highly prone to be fallacious due to the adoption of an insufficient security model which fails to capture all the realistic capabilities of the adversary or due to a flawed or non-tight security reduction, and the field of provable security is a much an art as a science. While formal methods are often misused and reductionist

security proofs are usually very intricate, turgid and prone to errors, particular care shall be given when conducting proof for an authentication protocol. To cope with the formal methods problems, this subsection is dedicated to present informal privacy and security analysis of the proposed protocol, which is focused on the privacy and security goals depicted in Section 2.3. For the CK threat model, we use the definition mentioned in Section 2.2. Table 2 shows the feature comparisons among the related protocols devised by Khatoun et al. in [34], Ostad-Sharif et al. in [35], Khan et al. in [38], Xu et al. in [40] and Alzahrani et al. in [41].

Table 2. Privacy and security feature comparison result.

Feature \ Protocol	Khatoun et al. [34]	Ostad-Sharif et al. [35]	Khan et al. [38]	Xu et al. [40]	Alzahrani et al. [41]	Proposed
SP1	O	O	O	O	O	O
SP2	O	O	O	O	O	O
SP3	O	O	O	O	O	O
SP4	O	O	X	X	X	O
SP5	X	X	X	X	X	O
PP1	O	O	O	X	O	O
PP2	O	O	O	X	X	O

SP1: mutual authentication, SP2: session key agreement, SP3: message freshness, SP4: perfect forward secrecy, SP5: attack resistance, PP1: anonymity, PP2: unlinkability.

[SP1] Mutual authentication: Authentication is performed between SN and HN mutually in the proposed protocol. Authentication is related to the messages from SN to HN and vice versa. SN needs to be authenticated by HN based on $\{X_{SN}, Y_{SN}, RID_S, T1_{SN}, PID_{AP}\}$, which is a message from SN to HN via AP. Only the legal SN could be authenticated by HN in the proposed protocol because a CK adversary needs to compute $RID_S = h(ID_{SN} || X_{SN} || Y_{SN} || S2_{SN} || T1_{SN})$, which needs knowledge on ID_{SN} and $S2_{SN}$ at the same time even if the adversary could get and use the previous session's X_{SN} and Y_{SN} . However, there is no way that the adversary could get them in the proposed protocol. HN needs to be authenticated by SN based on $\{r, NX_{SN}, NY_{SN}, C_{SN}, T2_{HN}\}$, which is a message from HN to SN via AP. Adversaries need to form a message, which could be validated by SN, especially C_{SN} validation that is related with knowledge of $q, ID_{SN}, j, X_{SN}', Y_{SN}'$ and $T2_{HN}$. However, the knowledge is related with KS_{HN} , which is the master key of HN. It means that the proposed protocol provides mutual authentication between SN and HN and there is no way that the adversary could succeed in the authentication process.

[SP2] Session key agreement: Session key is required to establish a secure channel between SN and HN to provide confidentiality on data. SN and HN agree on a session key $Ks = h(q || S1_{SN} || S2_{SN})$ after the successful authentication. There is no way that a CK adversary could get any information on Ks from the session messages $\{X_{SN}, Y_{SN}, RID_S, T1_{SN}\}, \{X_{SN}, Y_{SN}, RID_S, T1_{SN}, PID_{AP}\}, \{r, NX_{SN}, NY_{SN}, C_{SN}, T2_{HN}, NPID_{AP}, Z_{AP}\}$ and $\{r, NX_{SN}, NY_{SN}, C_{SN}, T2_{HN}\}$. The parameters of Ks are not exposed to any parameter in the messages. Especially, q is related to $r = q \oplus j$ but the adversary needs to know j to extract out the wanted value from r . However, the adversary could not get q from r due to the format of $j = ID_{SN} \oplus Y_{SN} \oplus X_{SN}$, which is related with the knowledge of KS_{HN} . Thereby, the proposed protocol provides a secure session key agreement only between SN and HN.

[SP3] Message freshness: There are two ways to provide message freshness in cryptographic protocol, which are based on challenge-response mechanism and timestamp mechanism. The proposed protocol uses a timestamp mechanism to cope with replay attacks because the network entity could be synchronized with a time when SA issues SN and AP for a PT during the registration phase. If a CK adversary wants to succeed in any attack against message freshness, the adversary needs to know and change timestamp-related values. From the session messages $\{X_{SN}, Y_{SN}, RID_S, T1_{SN}\}, \{X_{SN}, Y_{SN}, RID_S, T1_{SN}, PID_{AP}\}, \{r, NX_{SN}, NY_{SN}, C_{SN}, T2_{HN}, NPID_{AP}, Z_{AP}\}$ and $\{r, NX_{SN}, NY_{SN}, C_{SN}, T2_{HN}\}$, there are two integrity values $RID_S = h(ID_{SN} || X_{SN} || Y_{SN} || S2_{SN} || T1_{SN})$ and

$C_{SN} = h(q \parallel ID_{SN} \parallel j \parallel X_{SN}' \parallel Y_{SN}' \parallel T2_{HN})$ that the adversary needs to compute. If the adversary gets a proper current timestamp $T1_{SN}'$, the adversary should compute two new values of $RID_S = h(ID_{SN} \parallel X_{SN} \parallel Y_{SN} \parallel S2_{SN} \parallel T1_{SN}')$ and $C_{SN} = h(q \parallel ID_{SN} \parallel j \parallel X_{SN}' \parallel Y_{SN}' \parallel T1_{SN}')$. However, the two computations are impossible because the adversary needs to know the other parameters except $T1_{SN}'$ to compute RID_S and C_{SN} . Furthermore, each entity checks the freshness of the message using Δt each time they receive any message. So, the proposed protocol provides message freshness.

[SP4] Perfect forward secrecy: It is a very strong form of long-term security which guarantees that future disclosures of some long-term secret keys do not compromise past session keys [49]. It is widely accepted that the perfect forward secrecy can only be provided by asymmetric schemes. Nonetheless, there are a small number of existing symmetric-key protocols that provide secrecy [50–52]. The proposed protocol uses the dynamic authentication credential, which keeps evolving in sessions to achieve the perfect forward secrecy. In the proposed protocol, if an adversary has obtained the long-term key, K_{HN} , the adversary still cannot get the session key K_S . The reason is that after each successful session, the values HC_i , $S1_{SN}$ and $S2_{SN}$ will be updated by one-way hash function. Because of the one-wayness of the hash function, there is no way to get these values to compute the session key to the adversary. Therefore, the proposed protocol can provide perfect forward secrecy.

[SP5] Attack resistance: We could argue that any attack is successful if a CK adversary finds any mechanism to do various attacks, such as replay attack, impersonation attack and man-in-the-middle attack. Most of all, replay attack is tightly related with the message freshness. It means that any protocol with challenge-response or timestamp mechanism could cope with the attack. Messages in the proposed protocol are together with timestamp as the form of $T1_{SN}$ and $T2_{HN}$, respectively. Thereby, the proposed protocol is strong against replay attack. Impersonation attack is the second one we need to consider, which has a relationship with mutual authentication. As we mentioned in the mutual authentication, the adversary needs to form the first message $\{X_{SN}, Y_{SN}, RID_S, T1_{SN}\}$ to disguise as SN and the third message $\{r, NX_{SN}, NY_{SN}, C_{SN}, T2_{HN}, NPID_{AP}, Z_{AP}\}$ to masquerade as HN, respectively. However, they are related to the knowledge of KS_{HN} . So, the proposed protocol could cope with impersonation attacks. Man-in-the-middle attack is similar to an active eavesdropping in which the adversary makes independent connections with the network entities and relays messages between them to make them believe they are communicating directly to each other but in fact, the entire communication is controlled by the adversary. It is quite related to mutual authentication and confidentiality of parameters in the messages. Since we mentioned the mutual authentication provision from the proposed protocol, we will only consider confidentiality of the messages. There are only possibilities on knowing secret key-related information to legally registered SNs and HN but not any others. In the CK model, it is required that the generated session key from the protocol should not be compromised even in the case of ephemeral secrets leakage. In the proposed protocol, the ephemeral secrets are a_{SN} and q . Having access to these two, the adversary also needs to know both $S1_{SN}$ and $S2_{SN}$ to compute the session key K_S . Since only SN and HN know the values, the proposed protocol can withstand this attack. That is why any adversary could not get any useful information even if the adversary could tap into the communication link among SN, AP and HN. Thereby, the proposed protocol provides attack resilience. Finally, known session-specific temporary information attack should be considered in the protocol, which has an assumption that an adversary could get the ephemeral random number q to get the session key K_S since the attacker has no way to compute the long-term key KS_{HN} and one-time hash chain value HC_i . Moreover, the messages transmitted in the public channel are unhelpful to compute the session key K_S . Therefore, the proposed protocol has the ability to prevent the session-specific temporary information attack.

[PP1] Anonymity: Anonymity is defined as “the state of being not identifiable within a system.” Anonymity from a CK adversary’s perspective means that the adversary cannot identify any entity within a system. In security protocol, it is necessary to check identity-

related information in messages transmitted among system entities to consider anonymity. There are Y_{SN} , RID_S , NY_{SN} and C_{SN} , for ID_{SN} and PID_{AP} , $NPID_{AP}$ and Z_{AP} for ID_{SN} , respectively, in the messages, which has a relationship with the identity factor. Adversaries do not have any method to identify any entity from the parameters in the proposed protocol. To do so, the adversary needs to have knowledge of KS_{HN} , which is not feasible. As a result, the proposed protocol provides anonymity.

[PP2] Unlinkability: It has a meaning after a system with anonymity has been defined and the entities interested in linking by a CK adversary have been characterized. Unlinkability of two or more sessions of interest from the adversary's perspective means that within the system, the adversary cannot distinguish whether they are related or not. As we discussed on anonymity, session linkability is related to the identifier and the message freshness of session message parameters. Each parameter in the session messages has a relationship with the session-dependent random numbers of a_{SN} , $S1_{SN}$, $S2_{SN}$, q and na_{SN} and timestamps of $T1_{SN}$ and $T2_{HN}$ in the proposed protocol. It means that the proposed protocol uses session-dependent parameters to form messages to cope with unlinkability. So, the proposed protocol provides unlinkability.

As shown in Table 2, the proposed protocol satisfies all the security and privacy properties as we set our protocol design goal in Section 2.3. However, Khatoon et al.'s protocol does not provide SP5, especially against the known-session-specific temporary information attack as mentioned in [53]. Thereby, the adversary could compute the session key SK in Khatoon et al.'s protocol based on the session-specific temporary information, T_i , R_i , T_s and R_s , which are parameters to compute SK and are exposed on the public communication channel. As stated above, the attacker can compute L_s . Ostad-Sharif et al.'s protocol is weak against the denial-of-service attack, the password guessing attack and the stolen verifier attack [54]. So, Ostad-Sharif et al.'s protocol does not provide SP5 also. Furthermore, Khan et al.'s protocol has security weakness against the user impersonation attack, which is related to SP5 again [55]. Xu et al.'s protocol does not provide the replay attack since an attacker could configure a valid request by merging two session parameters by intercepting contents of the previous session and the current session parameters [41]. Alzahrani et al.'s protocol has a security weakness against the known-session-specific temporary information attack because it does not provide SP4 also. Furthermore, Xu et al.'s protocol and Alzahrani et al.'s protocol do not provide PP2 especially. In addition to this, Xu et al.'s protocol is not secure against the replay attack and the impersonation attack and does not provide PP1 due to the offline identity guessing attack feasibility [41].

5. Performance Results

In this section, we provide performance analysis focused on computation and communication overheads by providing comparisons with the related protocols in [34,35,38,40,41]. A dataset is developed to produce further testing and enhancements instead of spending a considerable amount of time, money and effort for data collection. 10 users were tested in the proposed protocol run for a total of 10 times. The experiment of the protocols was performed over ARM Microcontrollers MCU Mainstream Arm Cortex-M4 running on MCU 170 MHz with 128 KB of flash memory.

5.1. Computation Result

There are four phases in the proposed protocol, which are initialization phase, registration phase, authentication phase and identity modification phase. We will concentrate on the computation requirements of the authentication phase only from the proposed protocol because the phase is the most frequently used one. To facilitate computation analysis, we define the computational requirements of a one-way hash function as T_h , a symmetric key encryption and decryption as T_{sym} , an elliptic curve cryptosystem as T_{ecc} and a bilinear pairing operation as T_{bp} , respectively, but do not consider the overhead of the exclusive-or operations, which require a comparatively quite low overhead than any other operations. Table 3 shows the computational overhead comparison among the related protocols.

Table 3. Computation cost comparison result.

Entity \ Protocol	Khatoon et al. [34]	Ostad-Sharif et al. [35]	Khan et al. [38]	Xu et al. [40]	Alzahrani et al. [41]	Proposed
SN	$5T_h + 1T_{bp} + 1T_{sym} + 3T_{ecc}$	$7T_h + 2T_{ecc}$	$7T_h$	$4T_h$	$4T_h$	$4T_h$
AP	-	-	-	-	-	$1T_h$
HN	$4T_h + 1T_{bp} + 1T_{sym} + 2T_{ecc}$	$7T_h + 2T_{sym} + 2T_{ecc}$	$4T_h$	$6T_h$	$6T_h$	$9T_h$
Total	$9T_h + 2T_{bp} + 2T_{sym} + 5T_{ecc}$	$14T_h + 2T_{sym} + 4T_{ecc}$	$11T_h$	$10T_h$	$10T_h$	$14T_h$

From the experiment, we acquired the required time for T_h , T_{sym} , T_{ecc} and T_{bp} , which are approximately 0.08 ms, 0.14 ms, 4.31 ms and 14.48 ms, respectively. The proposed protocol requires 14 hash operations, which is a bit more expensive than the protocols in [38,40,41] but quite lower than the works in [34,35]. However, the protocols in [40,41] do not provide the privacy concerns as we discussed in Table 2. So, we could say that the computational overhead in the proposed protocol is for the sake of privacy-preserving. Especially, it is better to get less computational overhead on the patient side than the server side as the proposed protocol. However, Khan et al.’s protocol is opposite from the notion, which has a more burden to the patient’s side. Figure 5 shows the performance comparisons among the related protocols.

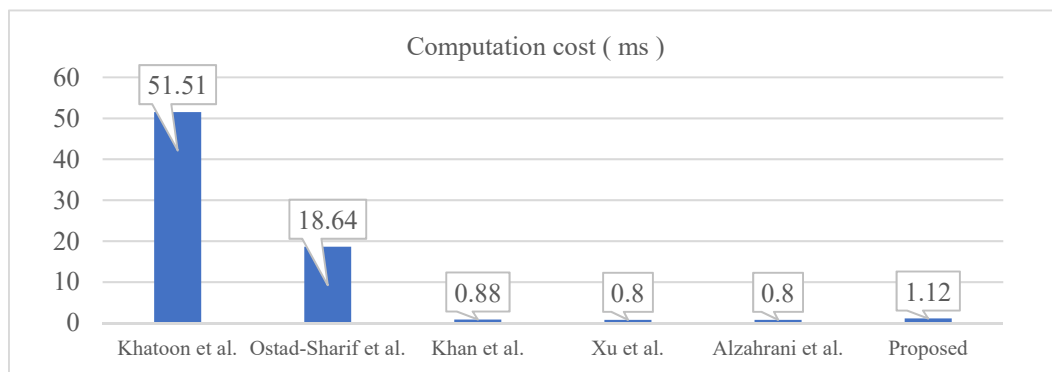


Figure 5. Computation cost comparison.

From Figure 5, we could know that the proposed protocol requires about 40% more computational overhead than the protocols in [38,40,41], which could be the overhead to provide unlinkability. However, the proposed protocol is relatively lightweight compared to the protocols in [34,35].

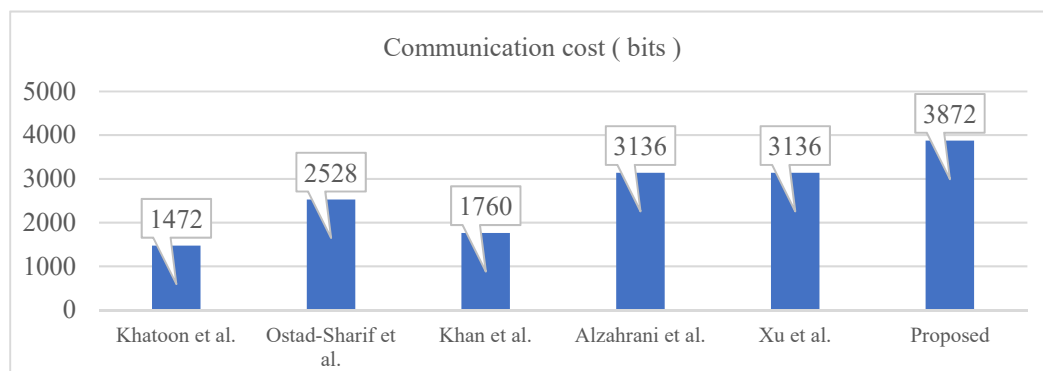
5.2. Communication Result

For the communication analysis, we assumed that the lengths of identity and random numbers are 128 bits each. However, we considered that the lengths for timestamp, hash function, symmetric key cryptosystem, elliptic curve cryptosystem and bilinear pairing are 32 bits, 160 bits, 128 bits, 256 bits and 256 bits, respectively. Table 4 shows a comparison for the communication cost among the related protocols.

Table 4. Communication cost comparison result.

Feature	Protocol	Khatoon et al. [34]	Ostad-Sharif et al. [35]	Khan et al. [38]	Xu et al. [40]	Alzahrani et al. [41]	Proposed
Message length	SN	832 bits	1408 bits	1120 bits	896 bits	896 bits	896 bits
	AP	-	-	-	1024 bits + 544 bits	1024 bits + 544 bits	1312 bits + 480 bits
	HN	640 bits	1120 bits	640 bits	672 bits	672 bits	1184 bits
	Total	1472 bits	2528 bits	1760 bits	3136 bits	3136 bits	3872 bits
Number of messages		2 messages	2 messages	2 messages	4 messages	4 messages	4 messages

Protocols of Khatoon et al., Ostad-Sharif et al. and Khan et al. require 2 messages with 1472 bits, 2528 bits and 1760 bits, respectively. However, protocols of Xu et al., Alzahrani et al. and the proposed one need 4 messages of 3136 bits, 3136 bits and 3872 bits, respectively. The first three protocols in Table 4 do not involve any intermediate entity between two end parties for the communication. That is why the communication requirements are less than those four other protocols. In addition to this, the proposed protocol requires about 700 bits more than Xu et al.'s protocol and Alzahrani et al.'s protocol due to the session-dependent dynamic identifier distribution to entities in the system. As shown in Figure 6, in contrast with the computational overhead, the proposed protocol requires the heaviest communicational overhead due to the usage of AP in between SN and HN, which is different from the other protocols.

**Figure 6.** Communication cost comparison.

6. Discussion

This section discusses challenges and solutions on the authentication protocol for WBAN based healthcare applications. After that, we will provide some future work.

6.1. Challenges and Solutions

Healthcare systems can provide an opportunity to meet the needs of individuals or households facing health difficulties. However, the healthcare system has an obligation to protect the privacy of patients [56]. And all participants in healthcare such as professionals of medical industries, always must be provide privacy with health data. Furthermore, healthcare professionals and medical industries around the globe are urged to fight against various security and privacy attacks on the healthcare system. WBAN based healthcare application shares some common functionalities with a typical computer network as it is a special type of network and also exhibits several unique characteristics that are specific to it. WBAN based healthcare application requires to guarantee security, privacy, data integrity and confidentiality of patient's EHR at all times. Towards the design of efficient cryptographic solution, there are more challenges in the WBANs than wired networks. They are the wireless nature of communication, resource inadequacy on SNs and very large and dense networks. Authentication is considered as the basic security building block for

any systems, which is a process by which the identity of a node in a network is verified and guarantees that the data or the control messages originate from an authenticated source. So, we will address some challenges and solutions for the authentication protocol.

The first challenge is to provide security in healthcare services that use the public network. Authentication protocol based on the public network is vulnerable against various attacks such as replay attack, impersonation attack and man-in-the-middle attack. The security issues could be overcome by utilizing various cryptographic primitives including asymmetric key cryptography, symmetric key cryptography, hash function and so on. Recently, researchers have been developing lightweight protocols, such as hash-based protocol and symmetric key cryptography-based protocol, to achieve feasibility on WBANs. Furthermore, designing authentication protocols with PUFs could help to resolve the security issues.

The second challenge is to preserve the privacy of network entities. Patient personal information is one of the most sensitive data in message transmission over the public network. The privacy issues could be dealt with by utilizing session-dependent information such as a one-time pseudonym for only the session usage. Recently, researchers have been deploying unidirectional hash chain values. A hash value from the chain is used only once and authentication protocol based on the value could provide unlinkability between sessions. In addition, cryptographic researchers should collaborate with healthcare professionals and medical industry workers to adopt and recognize various target field requirements from different backgrounds and aspects.

6.2. Future Work

In short, the proposed authentication protocol tries to generalize the process of mutual authentication and session key agreement for WBANs in healthcare applications. The proposed protocol takes full lightweight advantage of one-way hash function and exclusive-or operation to establish better security and privacy in solving authentication and session key establishment issues. In our future work, we aim to implement the proposed protocol in a real hospital environment with a big EHR database. We will focus on conducting experiments by optimizing patient side operational and communicational overhead of the proposed protocol to achieve better WBAN feasibility in terms of improved security and privacy. In addition, we will deploy a real-time adaptive artificial intelligence model on categorizing and analyzing EHR data to provide much richer patient healthcare services. Artificial intelligence can bring numerous benefits to the evolving of the healthcare industry. Based on artificial intelligence software, certain symptoms can be detected before the obvious symptoms of diseases such as lung cancer appear [57]. In addition, in the case of learned artificial intelligence, it can reduce the possibility of a doctor's misdiagnosis, to reducing patient anxiety [58]. Moreover, this research work will motivate researchers to pay more attention to security and privacy and explore the combination of other technologies, such as multimedia, robots and smart cities, to provide more convenient healthcare services to patients.

7. Conclusions

In this paper, we proposed a privacy-preserving authentication protocol for WBANs in healthcare applications. First of all, we set our design goals focused on 5 security properties and 2 privacy requirements, which are mutual authentication, session key agreement, message freshness, perfect forward secrecy, attack resistance, anonymity and unlinkability. To satisfy those features, we designed a new authentication protocol based on only two simple and lightweight operations, hash and exclusive-or. Especially, to provide 2 privacy requirements, the proposed protocol uses session-dependent pseudo identifiers for SN and AP. The formal and informal privacy and security analyses demonstrate the resistance of the proposed protocol against all sorts of privacy and security attacks. Especially, the privacy and security features of the proposed protocol are formally verified and validated based on BAN logic and ProVerif simulation tool. Performance analysis showed that the

proposed protocol has a reasonable overhead compared to the related previous protocols but still lightweight. We need to note that privacy-preserving is an important feature in healthcare service because healthcare information is sensitive. Nobody wants to expose their EHR-related information to others.

Author Contributions: Conceptualization, H.K.; methodology, H.K.; software, H.R.; validation, H.K. and H.R.; formal analysis, H.K.; writing—review and editing, H.R.; supervision, H.K.; project administration, H.K.; funding acquisition, H.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data could be downloaded with the following URL at <https://github.com/hs-kim-andre/healthcare.git>, accessed on 26 August 2021.

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

References

- Dua, A.; Kumar, N.; Das, A.K.; Susilo, W. Secure Message Communication Protocol among Vehicles in Smart City. *IEEE Trans. Veh. Technol.* **2018**, *127*, 4359–4373. [[CrossRef](#)]
- Roy, S.; Chatterjee, S.; Das, A.K.; Chappopadhyay, S.; Kumar, N.; Vasilakos, A.V. On the Design of Provably Secure Lightweight Remote User Authentication Scheme for Mobile Cloud Computing Services. *IEEE Access* **2017**, *5*, 25808–25825. [[CrossRef](#)]
- Bali, R.S.; Kumar, N.S. Secure clustering for efficient data dissemination in vehicular cyber-physical systems. *Future Gener. Comput. Syst.* **2016**, *56*, 476–492. [[CrossRef](#)]
- Li, X.; Liu, T.; Obaidat, M.S.; Wu, F.; Vijayakumar, P.; Kumar, N. A Lightweight Privacy-Preserving Authentication Protocol for VANETs. *IEEE Syst. J.* **2020**, *14*, 3547–3557. [[CrossRef](#)]
- Vijayakumar, P.; Azees, M.; Chang, V.; Deborah, J.; Balusamy, B. Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks. *Clust. Comput.* **2017**, *20*, 2439–2450. [[CrossRef](#)]
- Pradhan, B.; Bhattacharyya, S.; Pal, K. IoT-Based Applications in Healthcare Devices. *J. Healthcare Eng.* **2021**, *2021*, 6632599.
- Paek, J.; Gaglione, O.; Gnawali, O.; Vierira, M.A.M.; Hao, S. Advances in Mobile Networking for IoT Leading the 4th industrial Revolution. *Mob. Inf. Syst.* **2018**, *2018*, 8176158. [[CrossRef](#)]
- Malik, N.N.; Alosaimi, W.; Uddin, M.I.; Alouffi, B.; Alyami, H. Wireless Sensor Network Applications in Healthcare and Precision Agriculture. *J. Healthc. Eng.* **2020**, *2020*, 8836613. [[CrossRef](#)]
- Cho, S.; Kim, H. Secure Authenticated Key Agreement for Telecare Health Services using Ubiquitous IoT. *Int. J. Adv. Electron. Comput. Sci.* **2019**, *6*, 28–32.
- Zhang, N.; Ning, W.; Xie, T.; Liu, J.; He, R.; Zhu, B.; Mao, Y. Spatial Disparities in Access to Healthcare Professionals in Sichuan: Evidence from County-Level Data. *Healthcare* **2021**, *9*, 1053. [[CrossRef](#)]
- Park, B.; Lee, H. Healthcare Safety Nets during the COVID-19 Pandemic Based on Double Diamond Model: A Concept Analysis. *Healthcare* **2021**, *9*, 1014. [[CrossRef](#)]
- McDonald, Y.J.; Goldberg, D.W.; Scarinci, I.C.; Castle, P.E.; Cuzick, J.; Robertson, M.; Wheeler, C.M. Health Service Accessibility and Risk in Cervical Cancer Prevention: Comparing Rural Versus Nonrural Residence in New Mexico: Health Service Accessibility. *J. Rural. Health* **2017**, *33*, 382–392. [[CrossRef](#)] [[PubMed](#)]
- Kaluski, D.N.; Stojanovski, K.; McWeeney, G.; Paunovic, E.; Ostlin, P.; Licari, L.; Jakab, Z. Health insurance and accessibility to health services among Roma in settlements in Belgrade, Serbia—The journey from data to policy making. *Health Policy Plan.* **2015**, *30*, 976–984. [[CrossRef](#)] [[PubMed](#)]
- Ganann, R.; Sword, W.; Newbold, K.B.; Thabane, L.; Armour, L.; Kint, B. Influences on mental health and health services accessibility in immigrant women with post-partum depression: An interpretive descriptive study. *J. Psychiatr. Ment. Health Nurs.* **2020**, *27*, 87–96. [[CrossRef](#)] [[PubMed](#)]
- Cookson, R.; Propper, C.; Asaria, M.; Raine, R. Socio-Economic Inequalities in Health Care in England. *Fisc. Stud.* **2016**, *37*, 371–403. [[CrossRef](#)]
- Bisio, I.; Lavagetto, F.; Marchese, M.; Sciarrone, A. A smartphone-centric platform for remote health monitoring of heart failure. *Int. J. Commun. Syst.* **2015**, *28*, 1753–1771. [[CrossRef](#)]
- Kalid, N.; Zaidan, A.A.; Zaidan, B.B.; Salman, O.H.; Hashim, M.; Albahri, O.S.; Albahri, A.S. Based on Real Time Remote Health Monitoring Systems: A New Approach for Prioritization “Large Scales Data” Patients with Chronic Heart Diseases Using Body Sensors and Communication Technology. *J. Med Syst.* **2018**, *42*, 1–37. [[CrossRef](#)]

18. Wang, P.; Tsao, L.; Chen, Y.; Lo, Y.; Sun, H. "Hesitating and Puzzling": The Experiences and Decision Process of Acute Ischemic Stroke Patients with Prehospital Delay after the Onset of Symptoms. *Healthcare* **2021**, *9*, 1061. [[CrossRef](#)]
19. Rahman, M.Z.U.; Karthik, G.V.S.; Fathima, S.Y.; Lay-Ekuakille, A. An efficient cardiac signal enhancement using time–frequency realization of leaky adaptive noise cancelers for remote health monitoring systems. *Measurement* **2013**, *46*, 3815–3835. [[CrossRef](#)]
20. Majumder, S.; Mondal, T.; Deen, M.J. Wearable Sensors for Remote Health Monitoring. *Sensors* **2017**, *17*, 130. [[CrossRef](#)]
21. Gu, D.; Humbatova, G.; Xie, Y.; Yang, X.; Zolotarev, O.; Zhang, G. Different Roles of Telehealth and Telemedicine on Medical Tourism: An Empirical Study from Azerbaijan. *Healthcare* **2021**, *9*, 1073. [[CrossRef](#)]
22. Al-Janabi, S.; Al-Shourbaji, I.; Shojafar, M.; Shamsirband, S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egypt. Inform. J.* **2017**, *18*, 113–122. [[CrossRef](#)]
23. Liu, Q.; Mkongwa, K.G.; Zhang, C. Performance issues in wireless body area networks for the healthcare application: A survey and future prospects. *SN Appl. Sci.* **2021**, *3*, 1–19. [[CrossRef](#)]
24. Formica, D.; Schena, E. Smart Sensors for Healthcare and Medical Applications. *Sensors* **2021**, *21*, 543. [[CrossRef](#)] [[PubMed](#)]
25. Tovino, S.A. Privacy and Security Issues with Mobile Health Research Applications. *J. Law Med. Ethics* **2019**, *47*, 154–158.
26. Kim, H. Research Issues on Data Centric Security and Privacy Model for Intelligent Internet of Things based Healthcare. *ICSES Trans. Comput. Netw. Commun.* **2019**, *5*, 1–3. [[CrossRef](#)]
27. Kim, H. Data Centric Security and Privacy Research Issues for Intelligent Internet of Things. *ICSES Interdisciplinary Trans. Cloud Comput. IoT Big Data* **2017**, *1*, 1–2.
28. Vijayakumar, P.; Chang, V.; Deborah, L.J.; Balusamy, B.; Shynu, P.G. Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks. *Future Gener. Comput. Syst.* **2018**, *78*, 943–955. [[CrossRef](#)]
29. Vora, J.; Italiya, P.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Hsiao, K.-F. Ensuring Privacy and Security in E-Health Records. In Proceedings of the 2018 International Conference on Computer, Information and Telecommunication Systems, Colmar, France, 11–13 July 2018.
30. Zhu, J.; Ma, J. A new authentication scheme with anonymity for wireless environments. *IEEE Trans. Consum. Electron.* **2004**, *50*, 231–235.
31. Lee, C.C.; Hwang, M.S.; Liao, I.E. Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Trans. Ind. Electron.* **2006**, *53*, 1683–1687. [[CrossRef](#)]
32. Memon, I.; Hussain, I.; Akhtar, R.; Chen, G. Enhanced Privacy and Authentication: An Efficient and Secure Anonymous Communication for Location Based Service Using Asymmetric Cryptography Scheme. *Wirel. Pers. Commun.* **2015**, *84*, 1487–1508. [[CrossRef](#)]
33. Reddy, A.G.; Das, A.K.; Yoon, E.J.; Yoo, K.Y. A Secure Anonymous Authentication Protocol for Mobile Services on Elliptic Curve Cryptography. *IEEE Access* **2016**, *4*, 4394–4407. [[CrossRef](#)]
34. Khatoun, S.; Rahman, S.M.M.; Alrubaian, M.; Alamri, A. Privacy-Preserved, Provable Secure, Mutually Authenticated Key Agreement Protocol for Healthcare in a Smart City Environment. *IEEE Access* **2019**, *7*, 47962–47971. [[CrossRef](#)]
35. Ostad-Sharif, A.; Abbasinezhad-Mood, D.; Kikooghadam, M. An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC. *Int. J. Commun. Syst.* **2019**, *32*, e3913. [[CrossRef](#)]
36. Ali, Z.; Ghani, A.; Khan, I.; Chaudhry, S.A.; Islam, H.; Giri, D. A robust authentication and access control protocol for securing wireless healthcare sensor networks. *J. Inf. Secur. Appl.* **2020**, *52*. [[CrossRef](#)]
37. Burrows, M.; Abadi, M.; Needham, R. A logic of authentication. *R. Soc. Lond. Math. Phys. Eng. Sci.* **1989**, *426*, 233–271.
38. Khan, I.; Chaudhry, S.A.; Sher, M.; Khan, J.I.; Khan, M.K. An anonymous and provably secure biometric-based authentication scheme using chaotic maps for accessing medical drop box data. *J. Supercomput.* **2018**, *74*, 3685–3703. [[CrossRef](#)]
39. Aman, M.N.; Chua, K.C.; Sikdar, B. A light-weight mutual authentication protocol for IoT systems. In Proceedings of the 2017 IEEE Global Communications Conference, Singapore, 4–18 December 2017.
40. Xu, Z.; Xu, C.; Chen, H.; Yang, F. A lightweight anonymous mutual authentication and key agreement scheme for WBAN. *Concurr. Comput. Pract. Exp.* **2019**, *31*, e5295. [[CrossRef](#)]
41. Alzahrani, B.A.; Irshad, A.; Albeshri, A.; Alsubhi, K. A Provably Secure and Lightweight Patient-Healthcare Authentication Protocol in Wireless Body Area Networks. *Wirel. Pers. Commun.* **2021**, *117*, 47–69. [[CrossRef](#)]
42. Blanchet, B. Automatic Verification of Security Protocols in the Symbolic Model: The Verifier ProVerif. *Lect. Notes Comput. Sci.* **2013**, *8604*, 54–87.
43. Liu, B.; Han, B.; Zheng, H.; Liu, H.; Zhao, T.; Wan, Y.; Cui, F. Who Is the Most Vulnerable to Anxiety at the Beginning of the COVID-19 Outbreak in China? A Cross-Sectional Nationwide Survey. *Healthcare* **2021**, *9*, 970. [[CrossRef](#)]
44. Canetti, R.; Krawczyk, H. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels. In Proceedings of the EUROCRYPT 2001, Innsbruck, Austria, 6–10 May 2001; Springer: Berlin/Heidelberg, Germany, 2001; pp. 453–474.
45. Sarr, A.P.; Elbaz-Vincent, P.; Bajard, J.-C. A New Security Model for Authenticated Key Agreement. In Proceedings of the Security and Cryptography for Networks, Amalfi, Italy, 13–15 September 2010; Springer: Berlin/Heidelberg, Germany, 2010; pp. 219–234.
46. Xu, Z.; Luo, M.; Kumar, N.; Vijayakumar, P.; Li, L. Privacy-Protection Scheme Based on Sanitizable Signature for Smart Mobile Medical Scenarios. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8877405. [[CrossRef](#)]
47. Klumpp, M.; Hintze, M.; Immonen, M.; Ródenas-Rigla, F.; Pilati, F.; Aparicio-Martínez, F.; Çelebi, D.; Liebig, T.; Jirstrand, M.; Urbann, O.; et al. Artificial Intelligence for Hospital Health Care: Application Cases and Answers to Challenges in European Hospitals. *Healthcare* **2021**, *9*, 961. [[CrossRef](#)]

48. Wang, D.; He, D.; Wang, P.; Chu, C. Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment. *IEEE Trans. Dependable Secur. Comput.* **2015**, *12*, 428–442. [[CrossRef](#)]
49. Avoine, G.; Canard, S.; Ferreira, L. Symmetric-key Authenticated Key Exchange (SAKE) with Perfect Forward Secrecy. In Proceedings of the CT-RSA, San Francisco, CA, USA, 24–28 February 2020; Springer: Cham, Switzerland, 2020; pp. 24–28.
50. Bellare, M.; Yee, B.B. Forward-security in private-key cryptography. In Proceedings of the CT-RSA, San Francisco, CA, USA, 13–17 April 2003; Springer: Berlin/Heidelberg, Germany, 2003; pp. 1–18.
51. Brier, E.; Peyrin, T. A forward-secure symmetric-key derivation protocol—How to improve classical DUKPT. In Proceedings of the ASIACRYPT, Singapore, 5–9 December 2010; Springer: Berlin/Heidelberg, Germany, 2010; pp. 250–257.
52. Abdalla, M.; Bellare, M. Increasing the lifetime of a key: A comparative analysis of the security of re-keying techniques. In Proceedings of the ASIACRYPT, Kyoto, Japan, 3–7 December 2000; Springer: Berlin/Heidelberg, Germany, 2000; pp. 546–559.
53. Nikooghadam, M.; Admintoosi, H. Cryptanalysis of Khatoon et al.’s ECC-based Authentication Protocol for Healthcare System. *arXiv* **2019**, arXiv:190608424N.
54. Li, W.; Wang, P. Two-factor authentication in industrial Internet-of_things: Attacks, evaluation and new construction. *Future Gener. Comput.* **2019**, *101*, 694–708. [[CrossRef](#)]
55. Babamir, F.; Kirci, M. Dynamic digest based authentication for client–server systems using biometric verification. *Future Gener. Comput. Syst.* **2019**, *101*, 112–126. [[CrossRef](#)]
56. Kaplan, B. How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales. *Camb. Q. Healthc. Ethics* **2016**, *25*, 312–329. [[CrossRef](#)]
57. Richens, J.G.; Lee, C.M.I. Improving the accuracy of medical diagnosis with causal machine learning. *Nat. Commun.* **2021**, *12*, 3923. [[CrossRef](#)]
58. How AI Technologies Accelerate Progress in Medical Diagnosis. Available online: <https://roboticsandautomationnews.com/2020/03/09/how-ai-technologies-accelerate-progress-in-medical-diagnosis/31184/> (accessed on 26 August 2021).