



Structural Vulnerabilities and Confirmed-Key Redesign of a Heterogeneous Hyperelliptic Curve Cryptography-Based Authentication Protocol for Wireless Body Area Networks

Haewon Byeon 

Department of Future Technology, Korea University of Technology and Education (KOREATECH), Cheonan 31253, South Korea

Corresponding Author Email: bhwpuma@naver.com

Copyright: ©2026 The author. This article is published by IIETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/isi.310912>

ABSTRACT

Received: 3 April 2026

Revised: 25 August 2026

Accepted: 7 September 2026

Available online: 30 September 2026

Keywords:

wireless body area networks, hyperelliptic curve cryptography, authentication protocol, protocol vulnerability analysis, key confirmation, forward secrecy, formal verification

This study re-examines the heterogeneous hyperelliptic curve cryptography (HECC)-based authentication protocol proposed by Ullah et al. for wireless body area networks (WBANs). The published protocol is reconstructed as an explicit state machine under a Dolev-Yao active-channel model augmented with selective compromise. Knowledge accounting and stepwise counterexample traces reveal four structural weaknesses: the client cannot compute the published authentication term from its retained state, recorded one-pass messages are replayable because responder freshness is absent, previously established session keys can be recovered after disclosure of the application-provider long-term scalar, and stored controller data enable offline password testing when the user identity is known or guessed. A confirmed-key redesign is then specified by mapping each failed security invariant to a corresponding repair mechanism, including sender-computable proofs, bilateral ephemeral key derivation, responder authentication, explicit key confirmation, rotating single-use pseudonyms, and removal of password-equivalent server state. Scyther is used to verify secrecy, agreement, and synchronization properties of the abstracted three-message exchange. Under the legacy coefficients reported by Ullah et al., the redesigned protocol requires eight HECC multiplications, corresponding to 3.84 ms of dominant public-key computation, and transmits 208 bytes. These results establish analytical feasibility under the stated model, while hardware-level efficiency, post-compromise security, and deployment readiness remain subjects for further validation.

1. INTRODUCTION

Wireless body area networks (WBANs) have moved from a niche sensing concept to a practical component of remote and preventive care. Tiny wearable or implantable devices can continuously report electrocardiogram traces, pulse rate, motion, oxygen saturation, and medication-related indicators to nearby mobile gateways and hospital services, which makes WBANs central to broader Internet-of-Things healthcare infrastructures [1-4]. This clinical usefulness comes with a familiar problem. The same wireless links that support timely care also expose highly sensitive physiological data to eavesdropping, message manipulation, traceability, and impersonation attempts [5, 6]. Because WBAN devices operate with tight energy, storage, and bandwidth budgets, protocol designers often seek lightweight constructions, but the reduction of cost cannot come at the price of protocol soundness.

A long line of healthcare authentication work has attempted to balance this tension. Earlier schemes focused on telecare and cloud-assisted medical access [7-11], while later studies targeted anonymous authentication, certificateless signatures, signcryption, and conditional privacy for WBAN and Internet of Health Things (IoHT) environments [12-27]. These studies

clarified several recurring design pressures: user anonymity should not eliminate traceability for medical accountability; server assistance should not create catastrophic key escrow; password or device-factor protection should remain robust even when local memory is extracted; and session keys should not collapse when a long-term credential is revealed after the fact. Recent surveys confirm that authentication, privacy preservation, and secure key establishment remain unresolved research themes in WBAN security engineering [2-4, 6].

Against this background, Ullah et al. [28] proposed “Enabling Secure Communication in WBANs with Heterogeneous Authentication Scheme” and argued that a heterogeneous design using certificateless cryptography on the client side, identity-based logic on the receiver side, and hyperelliptic curve cryptography (HECC) could offer strong privacy and low computation overhead. The paper is attractive on first reading because it addresses a real operational setting: body-worn sensors, a personal digital assistant, an application provider (AP), and a trusted key-generation center cooperate over BLE, 5G, and hospital networks. The scheme of Ullah et al. [28] is also notable because it attempts to combine conditional privacy and lightweight HECC operations in a single framework, which is exactly the kind of integration resource-constrained healthcare deployments demand.

Our re-examination of Ullah et al. [28] leads to a different conclusion. Once the setup equations, pseudo-identity logic, and authentication transcript are reconstructed carefully, the protocol reveals structural weaknesses that are not peripheral. The client is instructed to compute a signature term with values that the setup phase defines as application-provider secrets. The session key depends on a client ephemeral scalar and an application-provider static secret in a way that prevents forward secrecy. The protocol is published as a one-pass exchange, yet it claims mutual authentication without a responder challenge or explicit key confirmation. In addition, the stored masking relation for the password becomes testable offline if controller memory is compromised and the real identity is known or guessed. These are not cosmetic issues. They affect executability, replay safety, privacy, and post-compromise resilience at the same time.

This paper makes four bounded contributions. First, it reconstructs the published equations and records, for every value, its creator, required knowledge, transmission path, and lifetime. Second, it defines an explicit active-channel and selective-compromise adversary and gives reproducible counterexample traces for executability, replay, long-term-key exposure, local-memory exposure, and linkability. Third, it maps each failed invariant to a specific repair while retaining heterogeneous client and application-provider roles. Fourth, it compares schemes under a common objective checklist and transparent operation-count and packet-size model. Because certificateless proofs, rotating pseudonyms, bilateral ephemeral exchange, and Hash-based Message Authentication Code (HMAC) confirmation are established mechanisms, the redesign is presented as a conservative engineering repair profile for the specific failures in Ullah et al. [28], not as a novel authentication protocol or primitive.

2. RELATED WORK

Healthcare authentication literature can be divided into four broad streams. The first stream covers early telecare and cloud-assisted medical access systems, where protecting credentials and preserving patient privacy were the dominant concerns. Chen et al. [7] introduced a privacy authentication scheme for cloud-based medical environments, and Chiou et al. [8] showed that the original design did not adequately protect confidentiality and message authentication, and then proposed an improved version. Li et al. [9] designed a two-factor network-based e-healthcare protocol, while He et al. and Wei et al. [10, 11] examined telecare medicine authentication under stronger attack assumptions. These studies established the importance of password robustness, session key secrecy, and medical-data confidentiality, but many of them still relied

on server-centric trust or limited-factor assumptions.

The second stream focuses directly on WBAN authentication. Wu et al. [13] proposed anonymous authentication for WBANs but relied on bilinear pairings that are heavy for body-worn devices. He et al. [14] later offered an anonymous WBAN authentication design with provable security, yet bilinear pairing remained a cost concern. Ji et al. [15] moved toward certificateless conditional privacy preservation in big-data-enabled WBAN services, and Xie et al. [16] refined this line with CasCP, emphasizing efficiency and conditional privacy. Liao et al. [17] revisited certificateless signatures for remote WBAN authentication and exposed weaknesses in earlier formulations, while Li and Xu [18] proposed a more recent anonymous WBAN authentication protocol. These works collectively show that anonymous or certificateless design alone does not guarantee replay resistance, forward secrecy, or deployment-friendly state management.

The third stream addresses adjacent IoHT and wireless healthcare sensor settings, which are closely connected to WBAN deployments. Ullah et al. [19] designed an anonymous certificateless signcryption scheme for IoHT, and Noor et al. [20] proposed a secure channel-free anonymous certificateless signcryption method for WBAN. Khan et al. [21] explored online-offline certificateless signatures in IoHT, Chen et al. [22] introduced LAP-IoHT as a lightweight authentication protocol, and Ullah et al. [23] later investigated cross-domain access control for IoT-based WBANs. Chaudhry et al. [24] studied lightweight authentication in cloud-based IoT environments, while Ali et al. [25] designed a robust authentication and access-control protocol for wireless healthcare sensor networks. Kumar et al. [26] also considered certificateless aggregate signatures for healthcare wireless sensor networks. These protocols typically improve one or more dimensions, such as user anonymity, message size, or formal proof structure, but they also remind us that key-confirmation logic and memory-exposure resilience remain difficult to combine in one lightweight design.

Recent evidence sharpens this picture [29-31]. A 2024 survey classifies anonymous WBAN authentication mechanisms and their unresolved privacy and resource constraints [32]. Two 2025 studies develop biometric/asymmetric and fuzzy-extractor authentication schemes while again emphasizing formal analysis, constrained-device cost, and resistance to transcript attacks [33, 34]. These papers establish the current research status but are not direct heterogeneous-HECC baselines. The present work instead treats [28] as an executable state machine, derives counterexample traces from its equations, and links each repair to one failed invariant.

Table 1. Positioning of the present study relative to the cited authentication literature

Prior Line	Relationship to the Present Study
Certificateless WBAN [15-18]	Closest authentication baselines; the present work adds an executability-first reconstruction and explicit confirmed-key repair of Ullah et al. [28].
IoHT signcryption/access control [19-23]	Provides transferable credential and privacy mechanisms, but is not a direct heterogeneous HECC workflow baseline.
Exposure-aware healthcare authentication [24-27]	Motivates rotating identifiers and leak resilience; the redesign combines these with bilateral ephemeral derivation.
Recent and general healthcare/WBAN authentication [29, 30, 32-34]	Current contextual evidence; not direct heterogeneous-HECC performance baselines.
Target scheme [28]	Supplies the heterogeneous HECC equations and legacy cost coefficients subjected to structural analysis.

Note: WBAN = wireless body area network, HECC = hyperelliptic curve cryptography, IoHT = Internet of Health Things.

The cited works do not have identical scope. Certificateless WBAN schemes [15-18] are the closest authentication comparators; IoHT signcryption and access-control schemes [19-23] contribute transferable credential-management ideas; and [29, 30, 32-34] provide contextual evidence rather than direct HECC baselines. Table 1 makes these boundaries explicit and avoids treating unlike security objectives as interchangeable performance targets.

3. METHODOLOGY

3.1 Study design and reconstruction

The unit of analysis is the protocol transcript and persistent state reported in Ullah et al. [28]. We transcribed the setup, registration, pseudonym, authentication, and key-derivation equations without adding unreported messages. For each symbol, we recorded its domain, creator, initial owner, required inputs, transmitted form, storage location, and lifetime. An equation was marked executable only when its sender possessed every non-public input at that step. This knowledge-accounting rule separates a notation error from a protocol step that cannot be produced as specified.

3.2 Adversary model and scope

We use a Dolev-Yao active-channel adversary [31] augmented by selective compromise. Capability A1 permits interception, delay, deletion, modification, replay, and injection on BLE, gateway, 5G, and hospital links. A2 permits a snapshot of controller records, including the stored tuple defined by Ullah et al. [28]. A3 permits delayed disclosure of the AP long-term scalar after a target session has ended. A4 permits guessing structured client identities and dictionary passwords. A1 may be combined with either A2 or A3. The core model does not grant simultaneous access to both endpoint ephemeral scalars during the target run, compromise of the KGC master secret, or the ability to invert hashes, forge HMAC without its key, or solve the discrete-logarithm/Computational Diffie-Hellman problem in the selected group. These exclusions define the boundary of every security statement below.

3.3 Invariants and counterexample procedure

Six invariants are evaluated: P1 sender executability; P2 client-to-AP origin authentication; P3 responder authentication with explicit key confirmation; P4 session-specific replay rejection; P5 non-recovery of an archived session key after delayed long-term-key disclosure; and P6 resistance to offline local-factor testing and routine cross-session linkage. Algorithm 1 fixes the trace-generation rule used in Section 4.2. A trace is a counterexample when an honest step is not executable, an unauthorized transcript is

accepted, or a protected value becomes computable under A1–A4.

Algorithm 1. Adversarial trace generation for security property verification

TraceGen (protocol P , property P_k , capability A_m):

- (1) construct S_0 from each value's owner, inputs, transmitted form, storage, and lifetime;
 - (2) execute the honest transcript and reject a send step if its sender lacks an input (Trace E);
 - (3) apply A_m to record/replay a transcript (R), disclose a delayed long-term key (F), snapshot and test local-factor state (P), or compare persistent identifiers (U);
 - (4) recompute the receiving verification state;
 - (5) return the minimal accepted or disclosure trace and the failed invariant, otherwise return no counterexample within A_m .
-

3.4 Machine-checked symbolic validation

ProVerif is efficient for unbounded Horn-clause analysis, Tamarin is suited to mutable state and rich equational theories, and AVISPA offers multiple symbolic backends. Scyther 1.3.0 was selected here because its role-based model directly checks secrecy, liveness, weak agreement, non-injective agreement, and non-injective synchronization for the three-message exchange [35].

The model represents the HECC shared-secret step by ideal one-way encapsulation of two fresh contributions and binds PID, both roles, and both contributions into role-separated confirmations. With the unbounded option, all 10 client/AP claims returned Ok with proof of correctness. This machine-checked result supports network-level secrecy, agreement, synchronization, and confirmation only; it does not verify HECC algebra, password recovery, pseudonym-database behavior, side channels, or post-compromise forward secrecy.

3.5 Reproducible cost and communication model

The efficiency analysis is deterministic. To reproduce the legacy comparison, we retain the coefficients used by Ullah et al. [28]: one HECC multiplication $T_{HECC} = 0.48$ ms and one ECC multiplication $T_{ECC} = 0.97$ ms. Those coefficients came from the MIRACL-based environment reported by Ullah et al. [28] (2.0 GHz Intel Core i7-4510U, 8 GB RAM, Windows 7, and up to 1,000 primitive-level trials); they are source inputs, not new measurements by this study.

For scheme s , the dominant arithmetic cost is $C_s = n_{HECC,s} T_{HECC} + n_{ECC,s} T_{ECC}$. Hashes and HMACs are reported symbolically because the compared papers do not supply a common benchmark for them. Communication cost is the sum of transmitted fields under the byte lengths in Table 2. No stochastic simulation, repeated protocol run, confidence interval, or significance test is claimed. The unsupported simultaneous-client extrapolation in the earlier version has therefore been removed.

Table 2. Explicit assumptions for the reproducible analytical evaluation

Parameter	Specified Value/Rule
Security target	Conditional 128-bit target; requires vetted genus-2 parameters and constant-time implementation. Legacy timings are comparison inputs only.
Group representation	Prime-order genus-2 subgroup $q \geq 2^{256}$; generic Pollard-rho work $O(\sqrt{q})$, with $\sqrt{q} \geq 2^{128}$; curve-specific security must also be reviewed.
Hashes and confirmation	SHA-256; HMAC-SHA-256 truncated to a 16-byte online tag.

Online fields	PID 32 bytes; timestamp 8 bytes; compressed divisor 32 bytes; response scalar 32 bytes.
Proposed packet sizes	$M_1 = 104$ bytes; $M_2 = 88$ bytes; $M_3 = 16$ bytes; total = 208 bytes.
Legacy timing inputs	$T_{HECM} = 0.48$ ms; $T_{ECM} = 0.97$ ms, adopted from the MIRACL benchmark reported in reference [28].
Repetitions/statistics	Deterministic count model: one calculation per scheme; no random seed, variance estimate, or inferential test.
Client memory/deployment evidence	152-byte persistent state; code, public parameters, buffers, radio stack, and energy excluded. No WBAN sensor hardware was tested.

Note: WBAN = wireless body area network, HMAC = Hash-based Message Authentication Code.

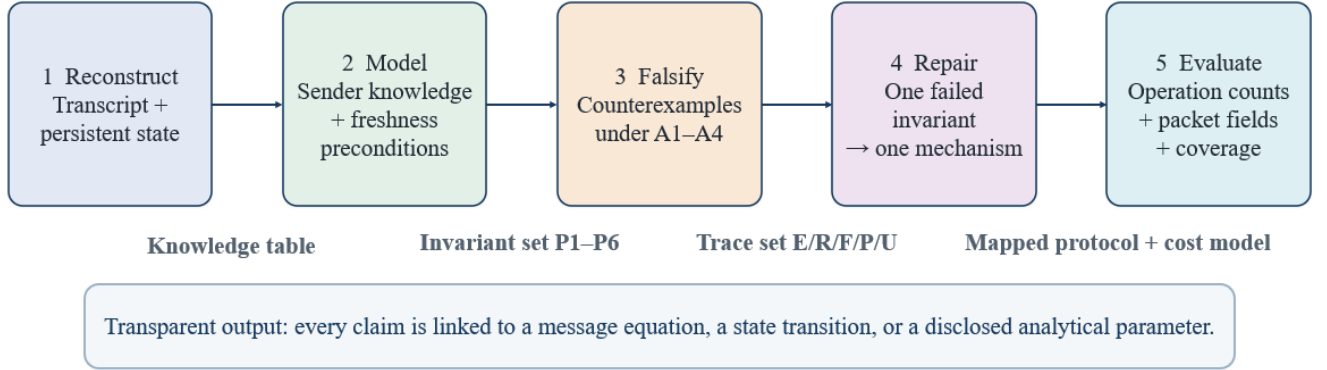


Figure 1. Analytical workflow used to reconstruct, attack, and redesign the heterogeneous wireless body area network (WBAN) authentication protocol

Figure 1 shows the sequential evidence chain: transcript reconstruction, knowledge/state modeling, manual counterexample generation under A1–A4, property-mapped repair, separate Scyther validation of the abstracted three-message exchange, and transparent cost accounting. The symbolic result complements rather than replaces the compromise and privacy analysis.

4. ANALYSIS OF THE PROTOCOL

4.1 Overview of the scheme

The original protocol of Ullah et al. [28] involves a client sensor, a personal gateway, an AP, and a key-generation center (KGC). Let $J_C(F_p)$ denote the genus-2 hyperelliptic-curve Jacobian used by the scheme, D a public generator of a subgroup of order q , and all lower-case secret scalars elements of $\mathbb{Z}_q$. The KGC selects hash functions $H_1 - H_4$, a master secret k , and $\alpha = kD$. The AP is assigned two secret scalars φ and τ and publishes $\eta = \varphi D$ and $Y = \tau D$. A client selects σ_i , forms $S_i = \sigma_i D$, and sends $(S_i, \text{RID}_i, \text{PW}_i)$ to the KGC over the protected registration channel.

For registration, the KGC selects θ_i and computes $h_i = \theta_i D$, $E_i = H_1(\text{RID}_i) \oplus H_1(\text{PW}_i)$, $\ell_i = H_2(kS_i, T_{\text{limit},i}, h_i)$, $\text{PID}_i = \text{RID}_i \oplus \ell_i$, $J_i = H_3(\text{PID}_i, S_i, h_i, T_{\text{limit},i})$, and $\Omega_i = \theta_i + kJ_i \bmod q$. It stores $(\text{PID}_i, S_i, h_i, T_{\text{limit},i}, \Omega_i, E_i)$ in controller memory. The client retains (Ω_i, σ_i) . Because PID_i and its masking inputs are fixed after registration, the identifier is not rotated per session.

In the published online phase, the client selects χ_j , computes $Q_j = \chi_j D$, $\text{SK}_j = \chi_j \eta$, $r_j = H_3(Q_j S_i, T_{\text{limit},i}, h_i, \text{PID}_i)$, and is instructed to form $s_{\text{auth},j} = \varphi + \tau + r_j \chi_j \bmod q$. It sends $M_{1,j} = (Q_j, r_j, s_{\text{auth},j})$. The AP accepts when $s_{\text{auth},j} D = Y + \eta + r_j Q_j$ and derives $\text{SK}_j = \varphi Q_j$. Thus, the specified transcript is a one-pass client-to-AP message. For contrast, Figure 2 previews the redesigned entity separation and the $M_1 - M_2 - M_3$ confirmed-key exchange

detailed in Section 5; it does not depict an extra message that exists in the original scheme.

4.2 Identified vulnerabilities

Trace E (executability) begins with the client state $\{\Omega_i, \sigma_i, S_i, h_i, \text{public parameters}\}$. The value $s_{\text{auth},j}$ requires φ and τ , but Ullah et al. [28] assigned both scalars exclusively to the AP. Therefore, the client cannot produce $M_{1,j}$ from its state. If φ and τ are instead disclosed to every client, any registered client can emulate the AP contribution. The verification equality depends on these same terms, so the inconsistency cannot be repaired by renaming a variable. Property P_1 fails.

Trace R (replay) has four steps. First, the adversary records an accepted $M_{1,j} = (Q_j, r_j, s_{\text{auth},j})$. Second, the target AP completes the run but stores neither Q_j nor PID_i as consumed. Third, the adversary resends the same triple within $T_{\text{limit},i}$. Fourth, the AP evaluates the unchanged equality $s_{\text{auth},j} D = Y + \eta + r_j Q_j$ and derives the same key φQ_j . Because no AP nonce, per-session timestamp, or confirmation value enters $M_{1,j}$, the AP has no protocol-level basis for distinguishing the replay. Property P_4 fails.

Trace F (delayed AP-key compromise) also requires only permitted capabilities. The adversary records Q_j during session j and later obtains φ through A_3 . Since Q_j is public, it computes the archived key $\text{SK}_j = \varphi Q_j$ directly; recovery of χ_j is unnecessary. Accordingly, past sessions are recoverable after AP long-term-key disclosure, and property P_5 fails for the published key relation.

Trace P (offline password testing) starts with an A2 controller snapshot containing E_i . If RID_i is known from hospital records or guessed from its structured format, the adversary computes $\text{target}_i = E_i \oplus H_1(\text{RID}_i)$. For each dictionary candidate pw^* , it evaluates $H_1(\text{pw}^*)$ and accepts the candidate when $H_1(\text{pw}^*) = \text{target}_i$. The test is local and requires no interaction with the client or AP. The stored value is therefore password-equivalent under the stated identity-

knowledge condition, so the local-factor part of P_6 fails.

Trace U (linkability) follows from state reuse. $PID_i = RID_i \oplus \ell_i$ is fixed at registration and remains an input to r_j in every session. A passive observer cannot necessarily recover RID_i , but repeated use of the same public identifier or correlated transport metadata permits session linkage. The

KGC can also recompute ℓ_i and recover the identity. Conditional tracing may be legitimate in healthcare, but it must be separated from routine observer linkability. The published design does not provide that separation, so the unlinkability part of P_6 is not established. Figure 3 summarizes the five counterexample surfaces.

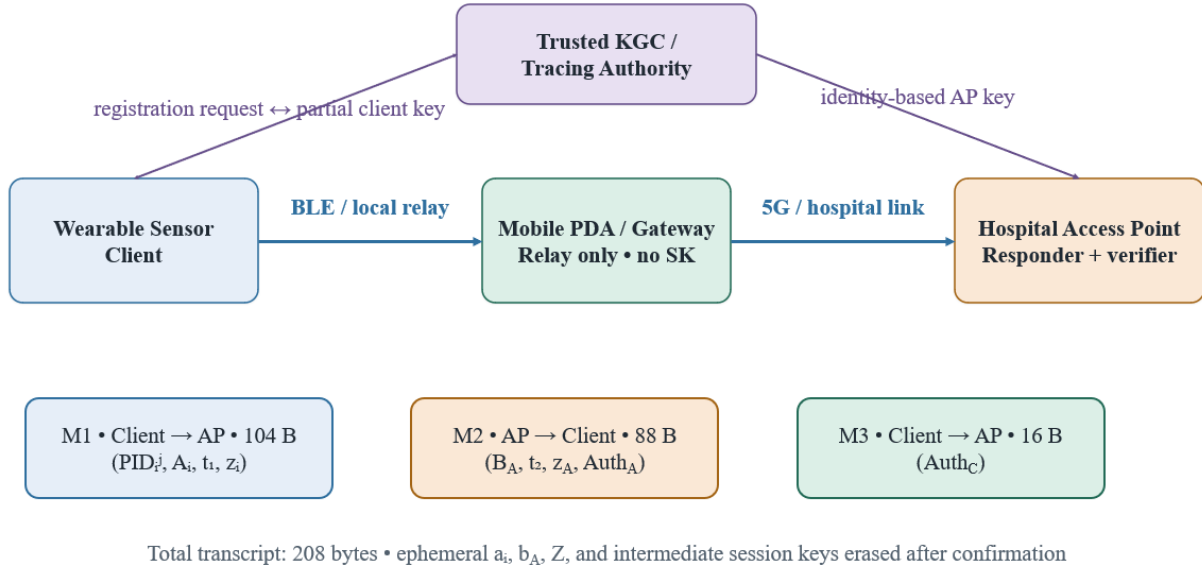


Figure 2. Entity roles and three-message flow of the proposed heterogeneous confirmed-key redesign

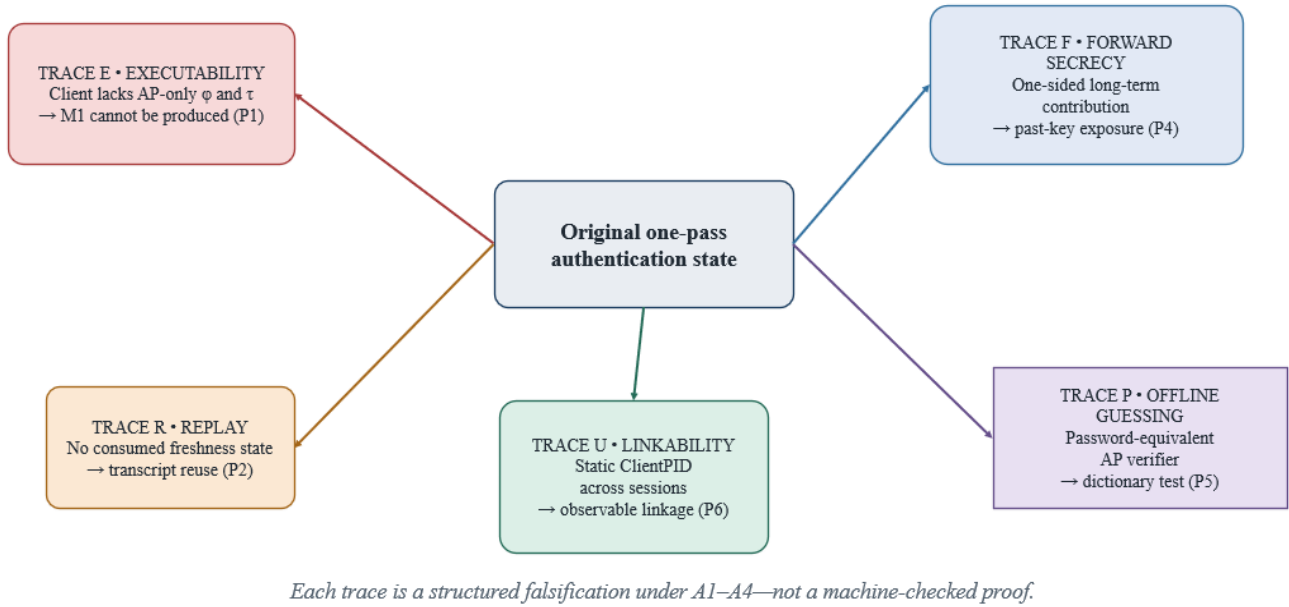


Figure 3. Attack-surface taxonomy derived from the original wireless body area network (WBAN) authentication equations and stored state

5. HETEROGENEOUS REDESIGN AND PROTOCOL SPECIFICATION

5.1 Enrollment and persistent state

The redesign removes password-equivalent material from the AP. During local enrollment, client i chooses a secret seed v_i and stores $T_i = v_i \oplus H_2(PW_i \parallel Bio_i \parallel salt_i)$ and $V_{loc,i} = H_3(v_i \parallel PW_i \parallel Bio_i)$. The tracing authority stores only an encrypted policy token $Trace_i = Enc_{K_{TA}}(RID_i \parallel v_i)$,

while the AP stores $PID_{root,i}$, the client verification base V_i , a bounded pseudonym lookup window, and consumed-counter state. A session pseudonym is $PID_i^j = H_4(v_i \parallel ctr_j \parallel ID_A)$. The counter increases monotonically, and successful use makes PID_i^j unavailable for later acceptance.

5.2 Online authentication pseudocode

Input: client state (v_i, sk_i, ctr_j) , AP state (d_A, V_i) , public

generator P , and freshness window Δ_t . Step 1 (client): verify local factors; sample a_i in $\mathbb{Z}_q$; compute $A_i = a_i P$, $e_i = H_5(\text{PID}_i^j \parallel A_i \parallel \text{ID}_A \parallel t_1)$, $z_i = a_i + e_i \text{sk}_i \bmod q$; send $M_1 = (\text{PID}_i^j, A_i, t_1, z_i)$. Step 2 (AP): reject stale t_1 or a consumed PID; verify $z_i P = A_i + e_i V_i$; sample b_A ; compute $B_A = b_A P$, $e_A = H_5(\text{ID}_A \parallel \text{PID}_i^j \parallel A_i \parallel B_A \parallel t_2)$, $z_A = b_A + e_A d_A \bmod q$, $Z = b_A A_i$, and $\text{SK}_j = H_6(Z \parallel \text{PID}_i^j \parallel \text{ID}_A \parallel A_i \parallel B_A \parallel t_1 \parallel t_2)$; send $M_2 = (B_A, t_2, z_A, \text{Auth}_A)$, where $\text{Auth}_A = \text{HMAC}_{\text{SK}_j}(\text{"AP"} \parallel \text{transcript})$. Step 3 (client): verify freshness, $z_A P = B_A + e_A V_A$, and Auth_A ; compute $Z = a_i B_A$ and SK_j ; send $M_3 = \text{Auth}_C = \text{HMAC}_{\text{SK}_j}(\text{"Client"} \parallel \text{transcript})$. Step 4 (AP): accept only after Auth_C verifies, then consume PID_i^j .

5.3 Property-to-mechanism mapping

The repair mapping now distinguishes evidence levels. P_1 is addressed because each proof uses only sender-held state; $P_2 - P_4$ are supported by the signed role transcript, responder freshness, role-separated confirmation tags, and consumed-PID state. The Scyther abstraction machine-checks secrecy, liveness, weak agreement, non-injective agreement, and synchronization for both roles. P_5 is designed to follow from $Z = a_i B_A = b_A A_i$ only when the Computational Diffie-Hellman assumption holds and a_i, b_A , and Z are erased. P_6 is designed to reduce offline testing and routine linkage by removing AP-side password-equivalent state and rotating PID_i^j . P_5 and P_6 remain analytical claims outside the present symbolic model and require computational and implementation validation.

5.4 Parameter, storage, and packet profile

The deployment profile targets 128-bit security conditionally. For a prime-order group with $q \geq 2^{256}$, generic Pollard-rho work scales as $O(\sqrt{q})$, with $\sqrt{q} \geq 2^{128}$; however, order size alone is insufficient, so the genus-2 curve and subgroup must also be generated and reviewed to exclude weak structure and faster curve-specific attacks, and the implementation must be constant-time. Compressed group elements, scalars, and PID_i^j are 32 bytes; timestamps are 8 bytes; and online HMAC-SHA-256 tags are 16 bytes. M_1, M_2 ,

and M_3 are 104, 88, and 16 bytes, respectively (208 bytes total). The client persistent fields total 152 bytes (six stated fields), while public parameters, code, message buffers, and radio-stack memory are excluded. Thus, suitability for a WBAN sensor is not established without device-specific RAM, flash, energy, and latency measurements.

6. PROPERTY TRACEABILITY AND REPRODUCIBLE COST ANALYSIS

6.1 Equivalent security objectives

The protocols in Table 3 have different trust assumptions, primitives, and online objectives. Accordingly, the table is scope-separated resource accounting, not an efficiency ranking: each number remains attached to the source protocol's stated objective set and the common legacy coefficient model. No superiority inference is made from the smallest operation count or packet size.

6.2 Criterion-level security traceability

Figure 4 is a criterion-level traceability matrix, not an aggregate score. For the redesign, a marked cell means that a stated equation, state update, and compromise boundary maps to the criterion. Only the abstracted network-level secrecy/agreement/synchronization claims were machine-checked in Scyther; the forward-secrecy and local-factor/linkability mappings remain analytical.

6.3 Deterministic operation and packet costs

Figure 5 reports the reproducible dominant-operation calculation. Applying the common legacy coefficients from Ullah et al. [28] gave $6 \times 0.48 = 2.88$ ms for the original HECC scheme, $6 \times 0.97 = 5.82$ ms for Ji et al. [15] and Xie et al. [16], and $8 \times 0.48 = 3.84$ ms for the public-key portion of the redesign. Five hashes and two HMAC evaluations are shown symbolically rather than assigned an unsupported common time. The 208-byte redesign transcript follows directly from the field lengths in Table 2. These values demonstrate the cost of the added security objectives under one transparent model; they are not end-to-end latency measurements.

Table 3. Scope-separated, non-ranking resource accounting under protocol-specific objectives

Protocol / Scope (Not Rank)	Explicitly Compared Online Objectives	Dominant Arithmetic Cost	Communication
Ji et al. [15]	Mutual authentication, replay defense, forward secrecy, and conditional privacy as reported by the source.	$6 T_{\text{ECM}} = 5.82$ ms	172 bytes
Xie et al. [16]	Mutual authentication, replay defense, forward secrecy, and conditional privacy as reported by the source.	$6 T_{\text{ECM}} = 5.82$ ms	217 bytes
Ullah et al. [28]	One-pass client claim; no responder freshness or explicit confirmation; archived keys recoverable after AP-key disclosure.	$6 T_{\text{HECM}} = 2.88$ ms	180 bytes
Engineering repair profile	Sender-computable client/AP proofs, bilateral ephemeral key, replay state, rotating PID, and explicit bilateral confirmation.	$8 T_{\text{HECM}} + 5 T_H + 2 T_{\text{MAC}}$; public-key part = 3.84 ms	208 bytes

6.4 Limitations

This study has four principal limitations. First, Scyther machine-checks only an idealized network-level abstraction;

HECC algebra, P5 post-compromise secrecy, P6 local-factor/linkability behavior, and a computational security reduction remain unverified. Second, the operation coefficients are inherited from the legacy MIRACL

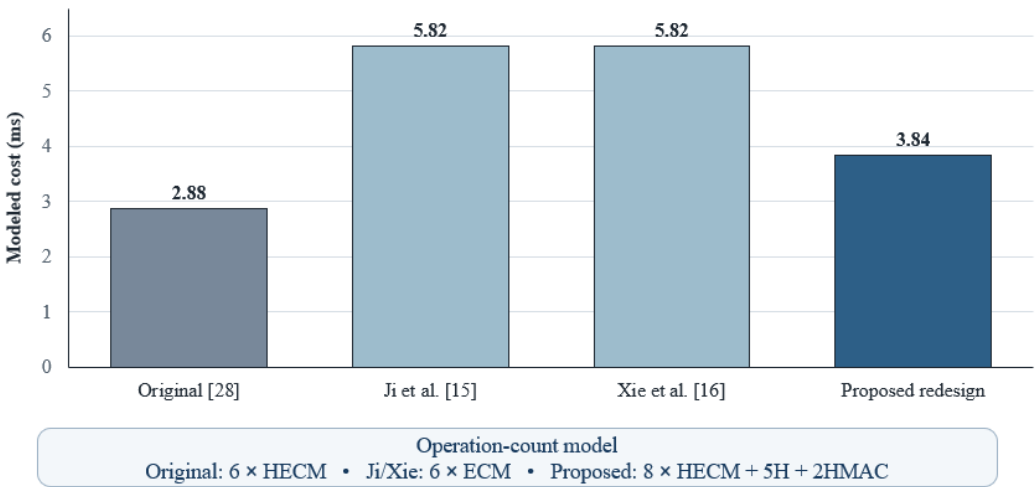
environment of Ullah et al. [28] and do not establish performance for a modern, validated 128-bit genus-2 implementation. Third, no wearable hardware, radio stack, hospital network, or clinical workflow was deployed, so the

152-byte persistent state excludes code, buffers, public parameters, energy, packet loss, and clock drift. Fourth, the deterministic counts do not support confidence intervals or significance testing.

Criterion	Original scheme [28]	Proposed redesign*
C1 Sender equation executable	NOT MET	MET*
C2 Responder proof + key confirmation	NOT MET	MET*
C3 Per-session freshness / replay state	NOT MET	MET*
C4 Bilateral ephemeral forward secrecy	NOT MET	MET*
C5 No server-side password equivalent	NOT MET	MET*
C6 Rotating public pseudonym	NOT MET	MET*

*Analytical satisfaction under the stated A1–A4 adversary model; not a machine-checked proof.

Figure 4. Criterion-level traceability for the original scheme and proposed redesign under the stated adversary model



$T_{HECM} = 0.48\text{ ms}$; $T_{ECM} = 0.97\text{ ms}$. Hash and HMAC costs remain symbolic to avoid unsupported timing assumptions.

Figure 5. Deterministic dominant-operation comparison using the legacy coefficients reported [28]

7. CONCLUSION

This study identifies reproducible structural failures in the heterogeneous HECC-based WBAN protocol of Ullah et al. [28] and specifies a property-mapped confirmed-key engineering repair. Its contribution is the combination of sender-knowledge accounting, explicit selective-compromise traces, a reproducible trace algorithm, and a mechanism-to-failure mapping-not a new primitive or authentication protocol. Under the stated model, the repair is designed to address sender computability, responder authentication, replay, bilateral ephemeral derivation, AP-side password-equivalent storage, and persistent pseudonyms. Scyther supports the abstracted network-level secrecy and agreement

claims, while P5 and P6 remain analytical. The 3.84-ms public-key count and 208-byte transcript indicate analytical feasibility only. Modern parameter validation and repeated sensor/gateway benchmarking remain necessary before deployment.

ACKNOWLEDGMENT

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Education (NRF-RS-2023-00237287 and 2026S1A5A01004224).

REFERENCES

- [1] Yin, Y.H., Zeng, Y., Chen, X., Fan, Y.J. (2016). The Internet of Things in healthcare: An overview. *Journal of Industrial Information Integration*, 1: 3-13. <https://doi.org/10.1016/j.jii.2016.03.004>
- [2] Narwal, B., Mohapatra, A.K. (2021). A survey on security and authentication in wireless body area networks. *Journal of Systems Architecture*, 113: 101883. <https://doi.org/10.1016/j.sysarc.2020.101883>
- [3] Hajar, M.S., Al-Kadri, M.O., Kalutarage, H.K. (2021). A survey on wireless body area networks: Architecture, security challenges and research opportunities. *Computers & Security*, 104: 102211. <https://doi.org/10.1016/j.cose.2021.102211>
- [4] Yaghoubi, M., Ahmed, K., Miao, Y. (2022). Wireless body area network (WBAN): A survey on architecture, Technologies, Energy Consumption, and Security Challenges. *Journal of Sensor and Actuator Networks*, 11(4): 67. <https://doi.org/10.3390/jsan11040067>
- [5] Lin, X.D., Lu, R.X., Shen, X.M., Nemoto, Y., Kato, N. (2009). Sage: A strong privacy-preserving scheme against global eavesdropping for e-health systems. *IEEE Journal on Selected Areas in Communications*, 27(4): 365-378. <https://doi.org/10.1109/JSAC.2009.090502>
- [6] Jabeen, T., Ashraf, H., Ullah, A. (2021). A survey on healthcare data security in wireless body area networks. *Journal of Ambient Intelligence and Humanized Computing*, 12(10): 9841-9854. <https://doi.org/10.1007/s12652-020-02728-y>
- [7] Chen, C.L., Yang, T.T., Chiang, M.L., Shih, T.F. (2014). A privacy authentication scheme based on cloud for medical environment. *Journal of Medical Systems*, 38(11): 143. <https://doi.org/10.1007/s10916-014-0143-9>
- [8] Chiou, S.Y., Ying, Z.Q., Liu, J.Q. (2016). Improvement of a privacy authentication scheme based on cloud for medical environment. *Journal of Medical Systems*, 40(4): 101. <https://doi.org/10.1007/s10916-016-0453-1>
- [9] Li, X., Niu, J.W., Karupiah, M., Kumari, S., Wu, F. (2016). Secure and efficient two-factor user authentication scheme with user anonymity for network based e-health care applications. *Journal of Medical Systems*, 40(12): 268. <https://doi.org/10.1007/s10916-016-0629-8>
- [10] He, D.B., Chen, J.H., Zhang, R. (2012). A more secure authentication scheme for telecare medicine information systems. *Journal of Medical Systems*, 36(3): 1989-1995. <https://doi.org/10.1007/s10916-011-9658-5>
- [11] Wei, J.H., Hu, X.X., Liu, W.F. (2012). An improved authentication scheme for telecare medicine information systems. *Journal of Medical Systems*, 36(6): 3597-3604. <https://doi.org/10.1007/s10916-012-9835-1>
- [12] Wu, F., Li, X., Sangaiah, A.K., et al. (2018). A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. *Future Generation Computer Systems*, 82: 727-737. <https://doi.org/10.1016/j.future.2017.08.042>
- [13] Wu, L.B., Zhang, Y.B., Li, L., Shen, J. (2016). Efficient and anonymous authentication scheme for wireless body area networks. *Journal of Medical Systems*, 40(6): 134. <https://doi.org/10.1007/s10916-016-0491-8>
- [14] He, D.B., Zeadally, S., Kumar, N., Lee, J.H. (2017). Anonymous authentication for wireless body area networks with provable security. *IEEE Systems Journal*, 11(4): 2590-2601. <https://doi.org/10.1109/JSYST.2016.2544805>
- [15] Ji, S., Gui, Z.Y., Zhou, T.Q., Yan, H.Y., Shen, J. (2018). An efficient and certificateless conditional privacy-preserving authentication scheme for wireless body area networks big data services. *IEEE Access*, 6: 69603-69611. <https://doi.org/10.1109/ACCESS.2018.2880898>
- [16] Xie, Y., Zhang, S.S., Li, X., Li, Y.G., Chai, Y. (2019). CasCP: Efficient and secure certificateless authentication scheme for wireless body area networks with conditional privacy-preserving. *Security and Communication Networks*, 2019: 5860286. <https://doi.org/10.1155/2019/5860286>
- [17] Liao, Y.J., Liu, Y.L., Liang, Y.K., Wu, Y., Nie, X.Y. (2020). Revisit of certificateless signature scheme used to remote authentication schemes for wireless body area networks. *IEEE Internet of Things Journal*, 7(3): 2160-2168. <https://doi.org/10.1109/JIOT.2019.2959602>
- [18] Li, C., Xu, C.X. (2022). Efficient anonymous authentication for wireless body area networks. *IEEE Access*, 10: 80015-80026. <https://doi.org/10.1109/ACCESS.2022.3180165>
- [19] Ullah, I., Alkhalifah, A., Rehman, S.U., Kumar, N., Khan, M.A. (2021). An anonymous certificateless signcryption scheme for Internet of Health Things. *IEEE Access*, 9: 101207-101216. <https://doi.org/10.1109/ACCESS.2021.3097403>
- [20] Noor, F., Kordy, T.A., Alkhodre, A.B., Benrhouma, O., Nadeem, A., Alzahrani, A. (2021). Securing wireless body area network with efficient secure channel free and anonymous certificateless signcryption. *Wireless Communications and Mobile Computing*, 2021: 5986469. <https://doi.org/10.1155/2021/5986469>
- [21] Khan, M.A., Rehman, S.U., Uddin, M.I., et al. (2020). An online-offline certificateless signature scheme for internet of health things. *Journal of Healthcare Engineering*, 2020: 1-10. <https://doi.org/10.1155/2020/6654063>
- [22] Chen, C.M., Chen, Z., Kumari, S., Lin, M.C. (2022). LAP-IoHT: A lightweight authentication protocol for the Internet of Health Things. *Sensors*, 22(14): 5401. <https://doi.org/10.3390/s22145401>
- [23] Ullah, I., Zeadally, S., Amin, N.U., Khan, M.A., Khattak, H. (2021). Lightweight and provable secure cross-domain access control scheme for Internet of Things-based wireless body area networks. *Microprocessors and Microsystems*, 81: 103477. <https://doi.org/10.1016/j.micpro.2020.103477>
- [24] Chaudhry, S.A., Irshad, A., Yahya, K., Kumar, N., Alazab, M., Zikria, Y.B. (2021). Rotating behind privacy: An improved lightweight authentication scheme for cloud-based IoT environment. *ACM Transactions on Internet Technology*, 21(3): 1-19. <https://doi.org/10.1145/3425707>
- [25] Ali, Z., Ghani, A., Khan, I., Chaudhry, S.A., Islam, S.H., Giri, D. (2020). A robust authentication and access control protocol for securing wireless healthcare sensor networks. *Journal of Information Security and Applications*, 52: 102502. <https://doi.org/10.1016/j.jisa.2020.102502>
- [26] Kumar, P., Kumari, S., Sharma, V., Sangaiah, A.K., Wei, J., Li, X. (2018). A certificateless aggregate signature scheme for healthcare wireless sensor network.

- Sustainable Computing: Informatics and Systems, 18: 80-89. <https://doi.org/10.1016/j.suscom.2017.09.002>
- [27] Chen, C.M., Li, Z., Chaudhry, S.A., Li, L. (2021). Attacks and solutions for a two-factor authentication protocol for wireless body area networks. *Security and Communication Networks*, 2021: 3116593. <https://doi.org/10.1155/2021/3116593>
- [28] Ullah, I., Khan, M.A., Abdullah, A.M., Noor, F., Innab, N., Chen, C.M. (2023). Enabling secure communication in wireless body area networks with heterogeneous authentication scheme. *Sensors*, 23(3): 1121. <https://doi.org/10.3390/s23031121>
- [29] Xie, Q.Y., Ding, Z.X., Xie, Q. (2023). A lightweight and privacy-preserving authentication protocol for healthcare in an IoT environment. *Mathematics*, 11(18): 3857. <https://doi.org/10.3390/math11183857>
- [30] Chen, C.M., Liu, S.S., Chaudhry, S.A., Chen, Y., Khan, M.A. (2022). A lightweight and robust user authentication protocol with user anonymity for IoT-based healthcare. *Computer Modeling in Engineering & Sciences*, 131(1): 307-329. <https://doi.org/10.32604/cmes.2022.018749>
- [31] Dolev, D., Yao, A.C. (1983). On the security of public key protocols. *IEEE Transactions on Information Theory*, IT-29(2): 198-208. <https://doi.org/10.1109/TIT.1983.1056650>
- [32] Wang, D., Zhou, J., Masdari, M., Qasem, S.N., Sayed, B.T. (2024). Security in wireless body area networks via anonymous authentication: Comprehensive literature review, scheme classification, and future challenges. *Ad Hoc Networks*, 153: 103332. <https://doi.org/10.1016/j.adhoc.2023.103332>
- [33] Mutlaq, K.A.A., Hasson, M.A., Abduljabbar, Z.A., et al. (2025). Anonymous wireless body area networks authentication protocol based on biometrics and asymmetric key cryptography. *Array*, 27: 100463. <https://doi.org/10.1016/j.array.2025.100463>
- [34] Wang, X., Xie, Y., Shui, D.Y., Ge, S.L. (2025). An improved biometric authentication and key agreement scheme based on fuzzy extractor for Wireless body area networks. *Journal of Information Security and Applications*, 91: 104047. <https://doi.org/10.1016/j.jisa.2025.104047>
- [35] Cremers, C.J.F. (2008). The scyther tool: Verification, falsification, and analysis of security protocols. In *Computer Aided Verification*. Berlin, Germany: Springer, pp. 414-418. https://doi.org/10.1007/978-3-540-70545-1_38