ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/363662844

Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks

Article *in* Journal of Sensor and Actuator Networks · September 2022

DOI: 10.3390/jsan11030055

CITATIONS
0

READS
3

7 authors, including:

Zaid Ameen Abduljabbar
Huazhong University of Science and Technology
96 PUBLICATIONS **256** CITATIONS

SEE PROFILE

Vincent O. Nyangaresi
University of Nairobi
96 PUBLICATIONS **450** CITATIONS

SEE PROFILE

Mustafa Alsibahee
Huazhong University of Science and Technology
46 PUBLICATIONS **144** CITATIONS

SEE PROFILE

Mudhafar JALIL JASSIM Ghrabat
Huazhong University of Science and Technology
8 PUBLICATIONS **48** CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:

LEACH-T LEACH Clustering Protocol Based on Three Layers View project

Structured Equation Modeling View project

All content following this page was uploaded by Zaid Ameen Abduljabbar on 19 September 2022.

The user has requested enhancement of the downloaded file.

Journal of
Sensor and Actuator Networks

MDPI

Article

Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks

Zaid Ameen Abduljabbar [1,2], Vincent Omollo Nyangaresi [3], Mustafa A. Al Sibahee [4,5,*], Mudhafar Jalil Jassim Ghrabat [6], Junchao Ma [4,*], Iman Qays Abduljaleel [7] and Abdulla J. Y. Aldarwish [1]

1 Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
2 Technical Computer Engineering Department, Al-Kunooze University College, Basrah 61001, Iraq
3 Faculty of Biological & Physical Sciences, Tom Mboya University, Homabay 40300, Kenya
4 College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
5 Computer Technology Engineering Department, Iraq University College, Basrah 61004, Iraq
6 IoT Research Center, Department of Pharmacy, Ashur University College, Baghdad 10047, Iraq
7 Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basrah 61004, Iraq
* Correspondence: mustafa@sztu.edu.cn or mustafa.alsibahee@iuc.edu.iq (M.A.A.S.); majunchao@sztu.edu.cn (J.M.)

Abstract: Wireless networks have continued to evolve to offer connectivity between users and smart devices such as drones and wireless sensor nodes. In this environment, insecure public channels are deployed to link the users to their remote smart devices. Some of the application areas of these smart devices include military surveillance and healthcare monitoring. Since the data collected and transmitted to the users are highly sensitive and private, any leakages can have adverse effects. As such, strong entity authentication should be implemented before any access is granted in these wireless networks. Although numerous protocols have been developed for this purpose, the simultaneous attainment of robust security and privacy at low latencies, execution time and bandwidth remains a mirage. In this paper, a session-dependent token-based payload enciphering scheme for integrity enhancements in wireless networks is presented. This protocol amalgamates fuzzy extraction with extended Chebyshev chaotic maps to boost the integrity of the exchanged payload. The security analysis shows that this scheme offers entity anonymity and backward and forward key secrecy. In addition, it is demonstrated to be robust against secret ephemeral leakage, side-channeling, man-in-the-middle and impersonation attacks, among other security threats. From the performance perspective, the proposed scheme requires the least communication overheads and a relatively low execution time during the authentication process.

Keywords: authentication; biometrics; chaotic maps; fuzzy extraction; key agreement

check for updates

Citation: Abduljabbar, Z.A.; Omollo Nyangaresi, V.; Al Sibahee, M.A.; Ghrabat, M.J.J.; Ma, J.; Qays Abduljaleel, I.; Aldarwish, A.J.Y. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. *J. Sens. Actuator Netw.* **2022**, *11*, 55. https://doi.org/10.3390/jsan11030055

Academic Editor: Chengwen Luo

Received: 26 August 2022
Accepted: 14 September 2022
Published: 19 September 2022

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

Copyright: © 2022 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/).

1. Introduction

Many wireless network technologies have been developed to facilitate data dissemination and the remote monitoring of physical phenomena. Among these technologies are Wireless Sensor Networks (WSNs), which comprise miniature and low-power devices referred to as sensor nodes [1]. These networks find applications in numerous fields such as in agriculture, disaster relief, military surveillance, transportation, industrial automation, wildlife and safety monitoring. In these environments, WSNs offer infrastructure-free data exchanges over shared network channels devoid of centralized access points [2]. A typical WSN comprises dynamic cooperating nodes that employ multi-hop information transfer [3]. According to [4], WSNs are robust networks that have self-managing and healing capabilities. As explained in [5], a WSN is basically made up of sensors, a gateway node (GWN) and the users. Compared with sensors, GWNs have high computation power,

energy and memory [5,6]. Due to their ease of deployment and their self-configuring and self-healing nature, WSNs' deployments are on the rise in multiple fields [7]. For instance, WSNs can monitor climatic conditions such as carbon dioxide, temperature, acidity, light and soil moisture [8].

Despite all the benefits that accrue from the deployment of WSNs, a number of challenges are encountered in these networks. According to [1], the provision of security during data transmission over public wireless channels is an uphill task. This problem is compounded by the fact that WSNs are typically deployed in untrusted environments [9]. As these sensors collect and transmit sensitive and private information, the privacy of users is at risk if leaked to malicious entities [10]. According to [1], attacks in WSN environments include smart card loss, sensor node capture and password guessing. However, authors in [4] identify Sybil, sinkhole and wormhole attacks as the main challenges. Authors in [11] have identified the broadcast nature of WSNs as being the source of numerous security attacks and vulnerabilities in these networks. Another challenge is that sensors in these networks are limited in terms of energy, memory, communication capabilities and processing power. As such, conventional encryption algorithms based on techniques such as Diffie and Hellman (DH) and Rivest–Shamir–Adleman (RSA) are unsuitable in WSNs due to the high overheads incurred during encryption or decryption [1,12].

It is evident that proper user authentication is required in WSN environments to offer security and privacy protection. Since the sensors are resource-constrained, these authentication schemes need to be lightweight. To offer enhanced privacy and thwart any privileged insider attacks, anonymity, untraceability and authorization must be assured during the authentication and data access process. After authentication, the users and the WSN entities must establish a session key to encipher the exchanged packets [1,13]. The specific contributions of this paper include the following:

- Fuzzy extraction is amalgamated with extended Chebyshev chaotic maps to generate authentication tokens that are shown to be session-specific for integrity enhancement.
- Symmetric encryption is deployed to generate temporary keys that are utilized during the authentication and key agreement phase to protect against backward and forward key secrecy compromise attacks.
- The mobile terminal and the gateway node negotiate a session key to encipher the payload exchanged over the public wireless channels.
- Extensive security analysis is carried out and shows that the proposed scheme offers strong mutual authentication and anonymity. In addition, our scheme is shown to be resilient against impersonation, side-channel, man-in-the-middle (MITM), secret ephemeral leakage and packet replay attacks.
- Performance evaluation is executed to show that the proposed scheme offers the best security features at relatively low execution time and communication costs.

The rest of this article is organized as follows: Section 2 presents related work regarding wireless network authentication and key agreement while Section 3 details the system model of the proposed scheme. On the other hand, Section 4 presents the comparative and evaluation results, while Section 5 concludes the paper.

2. Related Work

Numerous security and privacy-preserving techniques have been presented in the literature. However, most of these schemes still have security and privacy issues or have high overheads that render them unsuitable for WSN sensors. For instance, the remote user authentication protocol in [14] is susceptible to denial of service (DoS), off-line password guessing, sensor node capture and user impersonation attacks [15,16]. Similarly, the WSN security schemes in [17,18] cannot withstand off-line guessing attacks. On the other hand, the three-factor authentication in [19] does not offer sensor node anonymity and is vulnerable to de-synchronization attacks. The Chebyshev-chaotic-maps-based scheme is presented in [20], while cloud-centric authentication protocol is developed in [21]. Unfortunately, the scheme in [20,21] cannot withstand side-channeling attacks

through power analysis. The same security challenges are inherent in the chaotic-map-based protocol presented in [22]. As such, the passwords and identities stored in the smart card can be leaked. In addition, the protocol in [21] cannot offer perfect backward and forward key secrecy.

To protect data exchanged over WSNs, authors in [23] have presented a novel authentication scheme. However, as demonstrated by [24], this protocol is vulnerable to both de-synchronization and user forgery attacks. Similarly, the authentication and key agreement protocol introduced in [25] has security flaws [26,27]. Other sets of authentication protocols are based on three factors such as smart cards (SC), passwords and biometrics. In this regard, authors in [28–30] have introduced three-factor authentication (3FA) for enhancing security in wireless networks. However, the protocol in [30] cannot withstand user forgery and off-line password guessing attacks [31]. On the other hand, the schemes in [28,29] fail to offer both strong forward key security and offer anonymity [31]. To address these issues, an improved lightweight 3FA protocol is developed in [32]. Unfortunately, this scheme is still vulnerable to both user tracking and off-line guessing attacks [33]. Another 3FA protocol based on bio-hashing is introduced in [15]. However, this approach cannot uphold user anonymity and is vulnerable to both privileged insider and sensor node capture attacks [28]. To address the security challenges in 3FA schemes, other protocols based on techniques such as elliptic curve cryptography (ECC), exclusive-or (XOR), hash functions and biometric and machine learning, have been introduced. For instance, an ECC-based authentication protocol is presented in [34]. However, this protocol is not resilient against ephemeral secret leakage (ESL) attacks.

Apart from security and privacy issues, most of the conventional WSN authentication techniques have high false positives, long latencies or very high communication and computation costs. For instance, the scheme developed in [35] for malicious behavior detection in WSNs generates excessive false positives. On the other hand, the schemes in [36,37] enhance security but at the expense of increased latencies. On their part, the machine-learning-based protocols in [38–41] improve anomaly detection in networks. However, these schemes have high computational overheads and hence are not suitable for WSN sensors. On the other hand, the scheme developed in [42] upholds confidentiality, non-repudiation, authentication and integrity. Unfortunately, this protocol deploys bilinear pairing operations, which makes it computationally expensive [1,43] and hence not ideal for WSN environment. On their part, authors in [44] have developed a dynamic key management and authentication protocol based on bilinear pairing operations. Although this approach boosts security in hierarchical sensor networks, the deployed pairing operations inadvertently increase its computational complexity [45].

It is clear from the discussions above that the attainment of robust security and privacy at low computation, latency and communication costs is still an open challenge. In this paper, we leverage fuzzy extraction and extended Chebyshev chaotic maps to develop a scheme that is demonstrated to achieve robust security at the lowest communication costs and relatively lower computation overheads.

3. System Model

In this section, the mathematical primitives of the proposed scheme are discussed followed by the step-by-step discussion of the proposed scheme.

3.1. Mathematical Primitives

As already alluded to above, fuzzy extraction and extended Chebyshev chaotic maps are among the main building blocks of the proposed scheme. The mathematical formulations of these two concepts are elaborated upon in the sub-sections below.

3.1.1. Fuzzy Extraction

In biometric-based authentication systems, a fuzzy extractor is commonly deployed. This extractor has two functions, which include Gen and Rep. Given biometric information βio, the operations of these two functions are as follows:

1. (x_1, y_1) = Gen (β_{io}) implies that on receiving biometric β_{io}, function Gen(.) generates random string x_1 and auxiliary string y_1.
2. x_1 = Rep(β_{io}^{*}, y_1) implies that on receiving a noise biometrics β_{io}^{*} that is fairly similar to β_{io} and auxiliary string y_1 of β_{io}, function Rep(.) reproduces random string x_1.

3.1.2. Chaotic Maps

The proposed scheme is hinged on an extended Chebyshev polynomial (ECP), from which two computationally complex problems are derived. This ECP is based on the extended Chebyshev chaotic map. The two problems derived from ECP include the chaotic-maps-based Diffie–Hellman problem (CMDHP) and chaotic-maps-based discrete logarithm problem (CMDLP). Taking ń as a large prime number and λ1 and λ2 as positive integers, the ECP is defined as follows:

Definition 1. $C_r(\chi) = 2\chi\, C_{r-1}(\chi) - C_{r-2}(\chi) \bmod ń,\ r \geq 2.$

Definition 2. $C_0(\chi) = 1,\ \chi \in (-\infty, +\infty).$

Definition 3. $C_1(\chi) = \chi \bmod ń,\ \chi \in (-\infty, +\infty).$

On the other hand, the ECP satisfies the following condition:

$$C_{\lambda_1}\left(C_{\lambda_2}(\chi)\right) = C_{\lambda_2}\left(C_{\lambda_1}(\chi)\right) \bmod ń$$

During the security analysis of the authentication protocols, the ECP's CMDHP and CMDLP form the theoretical basis for guaranteeing the security of these protocols. These ECP problems are defined as follows:

1. CMDHP: Given χ, $C_{\lambda_1}(\chi)$ mod ń and $C_{\lambda_2}(\chi)$ mod ń, it is infeasible to derive $C_{\lambda_1}(C_{\lambda_2}(\chi))$ mod ń or $C_{\lambda_2}(C_{\lambda_1}\chi))$ using any polynomial time-bounded algorithm.
2. CMDLP: Given χ and $C_{\lambda_1}(\chi)$ mod ń, it is infeasible to compute integer λ_1 using any polynomial time-bounded algorithm.

3.2. Proposed Scheme

Wireless networks make it possible for users to interact with their smart devices in order to access and process data collected from sensors. To accomplish this, mobile terminals such as smart-phones are deployed. As such, in the proposed scheme, the mobile terminal (MT), sensor node (SN), gateway node (GWN) and the trusted authority (TA) are the main components, as shown in Figure 1. The communication between the sensor nodes and their gateway nodes is assumed to be secure. In addition, during the registration phase, the communication between the gateway node and the trusted authority is assumed to be through secure transmission channels. Similarly, the communication between the mobile terminal and the trusted authority during the registration phase is thought to be through secure channels.

In this architecture, the SN perceives the physical environment and forwards the collected data to the GWN for onward transmission to the remote user. On the other hand, the TA executes the registration of all GWNs and MTs before the commencement of data exchanges. Table 1 presents the symbols used in this paper.

The proposed scheme executes in five main phases, which include system initialization, device registration, authentication, key agreement and data exchange. The description of these phases is presented in the sub-sections below.

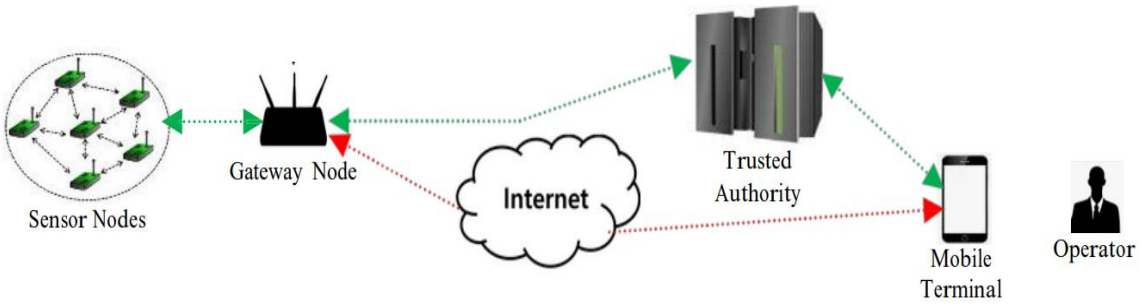

Figure 1. Network Architecture.

Table 1. Deployed symbols.

Symbol	Description
Ω_{TA}	TA's private key
$\mathcal{P}_{TA}$	TA's public key
ID_{OP}	Operator identity
SC_{OP}	Operator secret code
β_{OP}	Operator biometrics
$\hat{R}_i$	Random nonce
ID_G	GWN identity
SC_G	GWN secret code
Ω_G	GWN private key
Ψ	GWN temporary key
E_Q	Encryption using Q
D_Q	Decryption using Q
ϕ	Session key shared between MT and GWN
h(.)	Hashing operation
||	Concatenation operation
$\oplus$	XOR operation

3.2.1. System Initialization and Registration Phase

In this phase, the trusted authority (TA) initializes the system parameters, after which both the operator's MT and the GWN are registered at the TA. To accomplish MT registration, the operator identity, biometrics and password are input to this terminal. Afterwards, the MT submits its pseudonym P_{SN} to the TA through some secure channels. The TA then validates the supplied P_{SN} before storing the MT's security parameters in its database. The specific steps during initialization and registration are detailed below.

Step 1: The TA chooses a large prime number ń and random nonce $\hat{R}_1$ as Chebyshev chaotic map parameters. Next, the trusted authority TA generates nonce ΩTA as its private key before computing its public key $\mathcal{P}_{TA} = C_{\Omega_{TA}}(\hat{R}_1)$ mod ń, where ń is a large prime number. Taking m as the privacy message length, the TA selects two one-way hashing functions h_1: {0,1}* → $\{0,1\}^m$ and h_2: {0,1}* → $Z^*_{ń}$ before publishing parameter set $\{ń, \hat{R}_1, \mathcal{P}_{TA}, h_1, h_2\}$.

Step 2: The operator inputs identity ID_{OP} and secret code SC_{OP} to the mobile terminal MT before imprinting biometrics β_{OP} on the MT sensor. Thereafter, the MT chooses nonce $\hat{R}_2 \in Z^*_{ń}$ as its secret key before deriving security parameters $MT_{S1} = C_{\hat{R}_2}(\hat{R}_1)$ mod ń, $MT_{S2} = C_{\hat{R}_2}(\mathcal{P}_{TA})$ mod ń, $A_1 = ID_{OP} \oplus P_{SN}$ and $MT_{S3} = h_1(MT_{S2}) \oplus A_1$. The MT then sends registration request $MReg_{Req}$ to the TA accompanied by security parameters set $\{MT_{S3}, MT_{S1}\}$.

Step 3: After receiving the MT's registration request, the TA derives security parameters $MT_{S2}^* = C_{\Omega_{TA}}(MT_{S1})$ mod ń and $A_1^* = h_1(MT_{S2}^*) \oplus MT_{S3}$. It then extracts the operator inputs identity ID_{OP}^* and P_{SN}^* from A_1 before validating pseudonym P_{SN}^* by confirming whether $P_{SN}^* \stackrel{?}{=} P_{SN}$. Upon successful validation, the TA appends security set $\{ID_{OP}^*, MT_{S2}\}$

to its database. Finally, it transmits a registration successful $TReg_{SU}$ message to the MT, as shown in Figure 2.

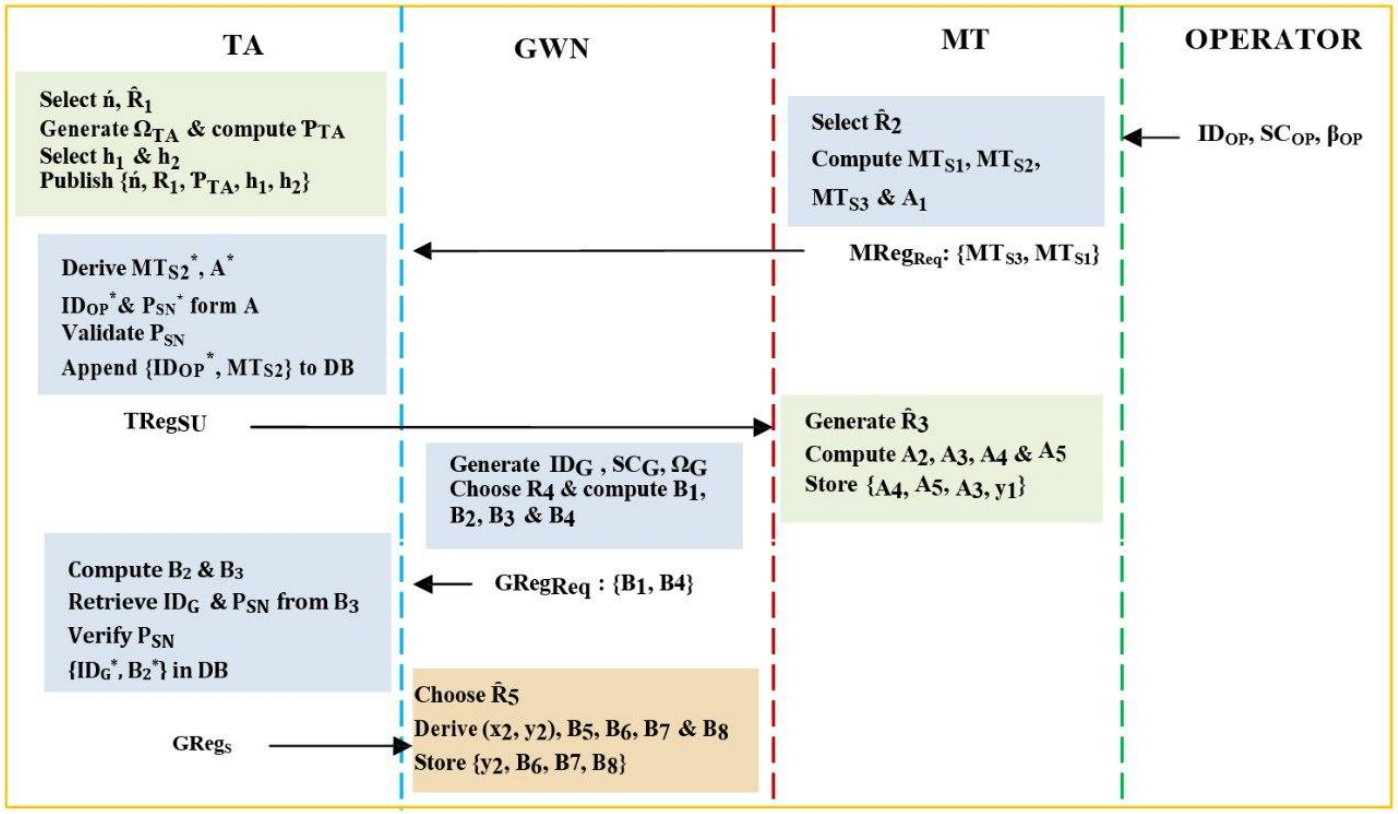

Figure 2. System initialization and registration message flows.

Step 4: On receiving $TReg_{SU}$ from the TA, the MT generates nonce $\hat{R}_3 \in Z_{ń}^*$ followed by the computation of $(x_1, y_1) = Gen(\beta_{OP})$, $A_2 = h_2(SC_{OP}, x_1, \hat{R}_3)$, $A_3 = A_2 \oplus \hat{R}_2$, $A_4 = \hat{R}_3 \oplus h_2(ID_{OP}, SC_{OP}, x_1)$ and $A_5 = h_2(ID_{OP}, A_2)$. Thereafter, it stores $\{A_4, A_5, A_3, y_1\}$ to its memory.

Step 5: During GWN registration, it generates identity ID_G, secret code SC_G and nonce Ω_G as its private key. It then chooses nonce $\hat{R}_4 \in Z_{ń}^*$ before computing $B_1 = C_{\hat{R}_4}(\hat{R}_1)$ mod ń, $B_2 = C_{\hat{R}_4}(\mathcal{P}_{TA})$ mod ń, $B_3 = (ID_G || P_{SN})$ and $B_4 = h_1(B_2) \oplus B_3$. Finally, the GWN sends registration request $GReg_{Req}$ to the TA together with parameter set $\{B_1, B_4\}$.

Step 6: On receiving $GReg_{Req}$ from the GWN, the TA computes $B_2^* = C_{\Omega_{TA}}(B_1)$ mod ń and $B_3^* = h_1(B_2^*) \oplus B_4$. Next, it retrieves ID_G^* and P_{SN} from B_3 before verifying P_{SN}^* by confirming whether $P_{SN}^* \stackrel{?}{=} P_{SN}$. Provided that this validation is successful, the TA stores security parameter set $\{ID_G^*, B_2^*\}$ in its database. This is followed by the transmission of a registration successful $GReg_{SU}$ message back to the GWN.

Step 7: After obtaining $GReg_{SU}$, the GWN chooses nonce $\hat{R}_5 \in Z_{ń}^*$ before deriving $(x_2, y_2) = (\Omega_G || \hat{R}_5)$, $B_5 = h_2(SC_G, x_2, \hat{R}_5)$, $B_6 = B_5 \oplus \hat{R}_4$, $B_7 = \hat{R}_5 \oplus h_2(ID_G, SC_G, x_2)$ and $B_8 = h_2(ID_G, B_5)$. Lastly, the GWN stores security parameter set $\{y_2, B_6, B_7, B_8\}$ in its memory.

These two phases can be summarized in the pseudo-code below:

BEGIN

1) Choose ń and $\hat{R}_1$.
2) Generate Ω_{TA} and compute $\mathcal{P}_{TA}$.
3) Select h_1 and h_2 and publish {ń, $\hat{R}_1$, $\mathcal{P}_{TA}$, h_1, h_2}.
4) Input ID_{OP} and SC_{OP} to the MT.
5) Imprint β_{OP} on the MT sensor.

6) Choose $\hat{R}_2$ and compute MT_{S1}, MT_{S2}, A_1 and MT_{S3}.
7) **MT** $\rightarrow$ **TA:** $\{MT_{S3}, MT_{S1}\}$
i) Derive MT_{S2}^* and A_1^*.
ii) Extract ID_{OP}^* and P_{SN}^* from A_1.
iii) Validate P_{SN}^*.
iv) **IF** validation is successful, **THEN:**
Append $\{ID_{OP}^*, MT_{S2}\}$ to database.
TA $\rightarrow$ MT: $TReg_{SU}$
ELSE: terminate session.
8) Generate $\hat{R}_3$ and compute (x_1, y_1), A_2, A_3, A_4 and A_5.
9) Store $\{A_4, A_5, A_3, y_1\}$ in memory.
10) Generate ID_G, SC_G and Ω_G.
11) Choose $\hat{R}_4$ and compute B_1, B_2, B_3 and B_4.
12) **GWN** $\rightarrow$ **TA:** $\{B_1, B_4\}$.
13) Compute B_2^* and B_3^*.
14) Retrieve ID_G^* and P_{SN} from B_3.
15) Verify PSN*.
16) **IF** verification is successful, **THEN:**
17) Store $\{ID_G^*, B_2^*\}$ in its database.
18) **TA** $\rightarrow$ **GWN:** $GReg_{SU}$
19) **ELSE:** terminate session.
20) Choose $\hat{R}_5$ and compute (x_2, y_2), B_5, B_6, B_7 and B_8.
21) Store $\{y_2, B_6, B_7, B_8\}$ in memory.
END

3.2.2. Mutual Authentication and Key Agreement Phase

During this phase, the operator supplies the valid identity, secret code and biometrics to the MT, after which a valid signature is generated. This signature is then validated by the TA, after which it derives a temporary key for the GWN. Next, the MT and GWN utilize the TA-generated temporary key to authenticate each other, as described in the steps below.

Step 1: The operator inputs identity ID_{OP} and secret code SC_{OP} before imprinting β_{OP} on the MT sensor. The MT then derives $x_1 = Rep(\beta_{OP}, y_1)$, $\hat{R}_3 = A_4 \oplus h_2(ID_{OP}, SC_{OP}, x_1)$ and $A_2 = h_2(SC_{OP}, x_1, \hat{R}_3)$. It then validates whether $A_5 \stackrel{?}{=} h_2(ID_{OP}, A_2)$. If this validation succeeds, the MT derives $\hat{R}_2 = A_2 \oplus A_3$. Next, it generates $\hat{R}_6 \in Z_{\acute{n}}^*$, which it uses to compute $D_1 = C_{\hat{R}_6}(\hat{R}_6) \bmod \acute{n}$, $D_2 = C_{\hat{R}_6}(\mathcal{P}_{TA}) \bmod \acute{n}$, $D_3 = h_1(D_2) \oplus A_1$, signature $MAC_M = h_2(D_2, A_1)$, $MT_{S2}^* = C_{\hat{R}_2}(\mathcal{P}_{TA}) \bmod \acute{n}$ and $D_4 = MAC_M + h_2(MT_{S2}, D_1)$. Lastly, the MT constructs authentication request $MAuth_{Req}$ and transmits it to the TA together with $\{D_1, D_4, D_3\}$.

Step 2: After receiving $MAuth_{Req}$, the TA derives $D_2^* = C_{\Omega_{TA}}(D_1) \bmod \acute{n}$ and $A_1^* = h_1(D_2^*) \oplus D_3$. Then the TA uses ID_{OP}^* to search for MT_{S2} so as to validate the MT through checking whether $D_4 - h_2(MT_{S2}^*, D_1) \stackrel{?}{=} h_2(D_2^*, A_1^*)$. If this validation is successful, the TA computes $D_5 = C_{\hat{R}_7}(\hat{R}_1) \bmod \acute{n}$, which it deploys to derive a temporary key for the GWN, $\Psi = h_2(D_2^*, A_1^*, MT_{S2}^*, ID_G^*, D_5)$. It then computes $D_6 = ID_{OP}^* \oplus P_{SN}^*$ and $MAC_T = h_2(D_1, \Psi, D_6)$. To obscure both D_6 and Ψ, the TA derives $E_1 = h_2(B_2^*, D_1) \oplus (\Psi || D_6)$. Finally, the TA constructs authentication request $GAuth_{Req}$, which is sent to the GWN together with parameter set $\{MAC_T, E_1, D_1\}$, as shown in Figure 3.

Step 3: Upon receiving GAuthReq, the GWN derives $(\Psi^* || D_6^*) = h_2(B_2, D_1) \oplus E_1$ followed by the confirmation of whether $MAC_T \stackrel{?}{=} h_2(D_1, \Psi^*, D_6^*)$. Provided that this verification is successful, the GWN generates nonce $\hat{R}_7 \in Z^*$ which it uses to derive $E_2 = C_{\hat{R}_7}(D_1) \bmod \acute{n}$, $E_3 = E_{h_2(E_2)}(A_1^*)$, $MAC_G = h_2(A_1^*, \Psi^*, D_5)$. Finally, the GWN composes authentication response $GAuth_{Res}$, which it transmits directly to the MT together with parameter set $\{D_5, E_3, MAC_G\}$.

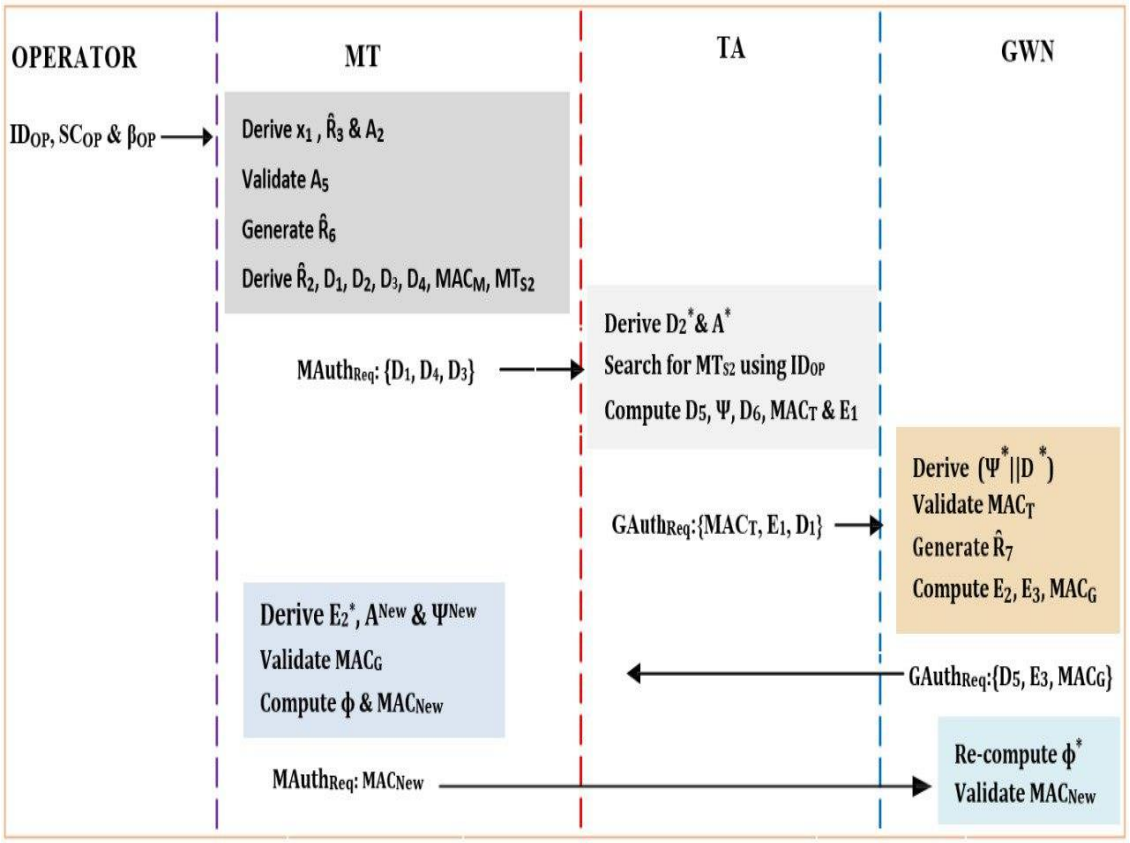

Figure 3. Authentication and key agreement message flows.

Step 4: After obtaining $GAuth_{Res}$, the MT derives $E_2^* = C_{\hat{R}_6}(D_5) \bmod \acute{n}$, $A_1^{New} = D_{h_2(E_2^*)}(E_3)$ and $\Psi^{New} = h_2(D_2, A_1, MT_{S2}, ID_G^*, D_5)$. It then checks whether $MAC_G \stackrel{?}{=} h_2(A_1^{New}, \Psi^{New}, D_5)$. If this verification is successful, the MT derives session key $\phi = h_2(E_2^*, \Psi^{New})$ to be utilized with the GWN for traffic enciphering. Lastly, it derives $MAC_{New} = h_2(\phi, A_1^{New})$ before sending it to the GWN together with authentication response message $MAuth_{Res}$.

Step 5: Once the GWN obtains $MAuth_{Res}$, it re-computes the session key $\phi^* = h_2(E_2, \Psi^*)$ and confirms whether $MAC_{New} \stackrel{?}{=} h_2(\phi^*, A_1^*)$. Provided that this verification is successful, the MT and GWN establish a secure channel between them and can now proceed to exchange network traffic. The mutual authentication and key agreement phase can be summarized in the following pseudo-code.

BEGIN
1) Input ID_{OP} and SC_{OP}.
2) Imprint β_{OP} to the MT.
3) Derive x_1, $\hat{R}_3$ and A_2.
4) Validate A_5.
5) **IF** validation is successful, **THEN:**
6) Compute $\hat{R}_2$ and generate $\hat{R}_6$.
7) Derive D_1, D_2, D_3, MAC_M, MT_{S2}^* and D_4.
8) **MT** $\rightarrow$ **TA:** $\{D_1, D_4, D_3\}$
9) Derive D_2^* and A_1^*.
10) Validate MT.
11) **IF** verification is successful, **THEN:**
12) Compute D_5, Ψ, D_6, MAC_T and E_1.
13) **TA** $\rightarrow$ **GWN:** $\{MAC_T, E_1, D_1\}$
14) **ELSE:** terminate session
15) Derive $(\Psi^* || D_6^*)$ and validate MAC_T.

16) **IF** validation is successful, **THEN:**
17) Generate $\hat{R}_7$ and derive E_2, E_3 and MAC_G.
18) **GWN → MT:** {D_5, E_3, MAC_G}
19) **ELSE:** terminate session.
20) Derive E_2^*, A_1^{New} and Ψ^{New}.
21) Validate MAC_G.
22) **IF** verification is successful, **THEN:**
23) Derive $\phi$and MAC_{New}.
24) **MT → GWN:** {$MAuth_{Res}$}
25) **ELSE:** terminate session.
26) Re-compute ϕ^* and authenticate MAC_{New}.
27) **IF** authentication is successful, **THEN:**
28) Initiate packet transfers.
29) **ELSE:** terminate session.
END

3.2.3. WSN Node–MT Communication Phase

This phase is triggered whenever the operator through the MT wants to access some data from the wireless sensor network nodes. To accomplish this, the operator supplies valid identity ID_{OP}, secret code SC_{OP} and biometrics β_{OP} on the MT sensor. This is followed by the generation of a legitimate signature for the operator, which is then transmitted to the TA for validation. After this, the TA stores some required information in its database. The steps followed during this phase are elaborated upon below.

Step 1: The operator inputs ID_{OP} and SC_{OP} to the MT before imprinting β_{OP} on the MT sensor. This invokes local authentication, in which the MT derives and validates whether $A_5 \stackrel{?}{=} h_2(ID_{OP}, A_2)$, as described in Step 1 of the mutual authentication and key agreement phase. If this local authentication is successful, the MT sends service access request $MServ_{Req}$ to the GWN.

Step 2: The GWN then derives x_2 = Rep (Ω_G, y_2), $\hat{R}_5 = B_7 \oplus h_2(ID_G, SC_G, x_2)$ and $B_5 = h_2(SC_G, x_2, \hat{R}_5)$. It then verifies whether $B_8 \stackrel{?}{=} h_2(ID_G, B_5)$. Provided that this validation is successful, the GWN computes $\hat{R}_4 = B_5 \oplus B_6$. It then employs nonce $\hat{R}_7$ to re-compute $D_5 = C_{\hat{R}_7}(\hat{R}_1) \bmod \acute{n}$, $F_1 = C_{\hat{R}_7}(\mathcal{P}_{TA}) \bmod \acute{n}$, $F_2 = h_1(F_1) \oplus A_1$, $MAC_G = h_2(F_1, A_1)$, $B_2 = C_{\hat{R}_4}(\mathcal{P}_{TA}) \bmod \acute{n}$ and $F_3 = MAC_G + h_2(B_2, D_5)$. Finally, the GWN sends access request $GServ_{Req}$ to the WSN node (SN) together with parameter set {D_5, F_2, F_3}.

Step 3: Upon receiving $GServ_{Req}$, the SN derives $F_1^* = C_{\Omega_{TA}}(D_5) \bmod \acute{n}$ and $A_1^* = h_1(F_1^*) \oplus F_2$. It then retrieves ID_G^* from its memory and searches for B_2^*. It then checks whether $F_3 - h_2(B_2^*, D_5) \stackrel{?}{=} h_2(F_1^*, A_1^*)$. If this verification is successful, the SN temporarily stores parameters {A_1^*, D_5} in its memory for any subsequent verification with this particular GWN. Finally, the SN packages the requested data and enciphers it using ϕbefore forwarding it to the GWN, which delivers it to the operator via the MT. This communication phase is summarized in the pseudo-code below.

BEGIN
1) Input ID_{OP} and SC_{OP} to the MT.
2) Imprint β_{OP} on the MT sensor.
3) Derives and validate A_5.
4) **IF** validation is successful, **THEN:**
5) **MT → GWN:** {$MServ_{Req}$}
6) **Derive** x_2, $\hat{R}_5$ and B_5.
7) **ELSE:** terminate session.
8) Verify B_8.
9) **IF** verification is successful, **THEN:**
10) Compute $\hat{R}_4$, D_5, F_1, F_2, MAC_G, B_2 and F_3.
11) **GWN → SN:** {D_5, F_2, F_3}
12) **Derive** $F_1^*$and A_1^*.

13) Retrieve ID_G^* and search B_2^*.
14) **ELSE:** terminate session.
15) Validate F_3 - h_2 (B_2^*, D_5).
16) **IF** validation is successful, **THEN:**
17) Temporarily store {A_1^*, D_5} in memory.
18) Package and encipher requested data using ϕ.
19) **SN → GWN → MT: {Data}**
20) **ELSE:** terminate session.
END

4. Comparative Analysis and Evaluation Results

In this section, the first part presents the security analysis of the proposed scheme. In the second part, the performance evaluation of the proposed scheme is given, together with a comparative evaluation of other related protocols.

4.1. Security Analysis

To show that the proposed scheme offers salient security and privacy features, seven hypotheses are formulated and proved as discussed below.

Hypothesis 1. *The proposed scheme offers both backward and forward key secrecy.*

Proof. Suppose that an adversary Å has obtained the secret parameters {D_5, E_3, MAC_G} and MAC_{New} exchanged between the MT and GWN. Here, $D_5 = C_{\hat{R}_7}(\hat{R}_1) \bmod \acute{n}$, $E_3 = E_{h_2(E_2)}(A_1^*)$, $MAC_G = h_2(A_1^*, \Psi^*, D_5)$ and $MAC_{New} = h_2(\phi, A_1^{New})$. The aim is to use these security parameters to compute session key $\phi = h_2(E_2^*, \Psi^{New})$, where $E_2^* = C_{\hat{R}_6}(D_5) \bmod \acute{n}$ and $\Psi^{New} = h_2(D_2, A_1, MT_{S2}, ID_G^*, D_5)$. However, without a knowledge of secret parameters ID_G^*, $\hat{R}_6$, D_2, A_1, MT_{S2} and $\hat{R}_7$, this session key can never be computed. In addition, an adversary is unable to derive $(C_{\hat{R}_7}(\hat{R}_1))$ or $C_{\hat{R}_7}((\hat{R}_1))$ devoid of $\hat{R}_6$ or $\hat{R}_7$. This is because these parameters are never transmitted over the network. □

Hypothesis 2. *Secret ephemeral leakage attacks are effectively thwarted in the proposed scheme.*

Proof. In the proposed scheme, session key $\phi = h_2(E_2^*, \Psi^{New})$ incorporates secret tokens Ψ and $C_{\hat{R}_6}$ $(C_{\hat{R}_7}(\hat{R}_1))$ among other parameters, where $\Psi = h_2(D_2^*, A_1^*, MT_{S2}^*, ID_G^*, D_5)$. Suppose that all these parameters including $\hat{R}_6$ and $\hat{R}_7$ are compromised. However, the adversary still needs to derive Ψ, which requires knowledge of GWN identity ID_G^*, D_2^*, A_1^* and MT_{S2}^*. Since all these security parameters are never sent over the communication channels, they cannot be eavesdropped by Å and hence the leakage of ephemerals Ψ, $C_{\hat{R}_7}(\hat{R}_1) \bmod \acute{n}$, $C_{\hat{R}_7}(D_1) \bmod \acute{n}$, $\hat{R}_6$ and $\hat{R}_7$ does not compromise the generated session key. □

Hypothesis 3. *The proposed scheme provides strong mutual authentication.*

Proof. Upon the input of valid operator identity ID_{OP}, secret code SC_{OP} and biometrics β_{OP}, the MT derives private key $\hat{R}_2 = A_2 \oplus A_3$, after which it generates signature $MAC_M = h_2(D_2, A_1)$. Thereafter, the TA authenticates the MT by checking this signature. This is achieved through checking whether $D_4 - h_2(MT_{S2}^*, D_1) \stackrel{?}{=} h_2(D_2^*, A_1^*)$. Meanwhile, the TA derives a temporary key for the GWN, $\Psi = h_2(D_2^*, A_1^*, MT_{S2}^*, ID_G^*, D_5)$. To securely transmit this temporary key to the GWN, the TA derives $E_1 = h_2(B_2^*, D_1) \oplus (\Psi \,||\, D_6)$. At the GWN, Ψ is deployed to generate signature $MAC_G = h_2(A_1^*, \Psi^*, D_5)$, which is utilized by the MT to authenticate the GWN and TA. This is achieved by checking whether $MAC_G \stackrel{?}{=} h_2(A_1^{New}, \Psi^{New}, D_5)$. Similarly, the MT generates signature $MAC_{New} = h_2(\phi, A_1^{New})$, which is employed by the GWN to authenticate the MT. This is executed by checking whether

$MAC_{New} \stackrel{?}{=} h_2(\phi^*, A_1^*)$. Consequently, strong mutual authentication between the MT and GWN, the MT and TA and the TA and GWN is attained. □

Hypothesis 4. *Side-channeling attacks are prevented in the proposed scheme.*

Proof. Suppose that an adversary Å manages to capture parameter set $\{A_4, A_5, B_6, y_1\}$ stored in the MT through power analysis. The goal of Å is to use these security tokens to derive ID_{OP}, SC_{OP} and β_{OP} by performing the following: $A_4 = \hat{R}_3 \oplus h_2(ID_{OP}, SC_{OP}, x_1)$, $A_2 = h_2(SC_{OP}, x_1, \hat{R}_3)$ and $A_5 = h_2(ID_{OP}, A_2)$. It is evident that all these computations require either the operator identity ID_{OP}, secret code SC_{OP} or biometric β_{OP}, which are unavailable in the MT's memory. Similarly, even if an adversary Å uses power analysis to obtain $\{B_7, F_1, B_6, y_2\}$ stored in GWN, all operator details cannot be obtained. □

Hypothesis 5. *The proposed scheme establishes a session key between the GWN and MT.*

Proof. After mutual authentication, the MT and GWN negotiate key $\phi = h_2(E_2^*, \Psi^{New})$ based on $\Psi^{New} = h_2(D_2, A_1, MT_{S2}, ID_G^*, D_5)$ and $C_{\hat{R}_6}(C_{\hat{R}_7}(\hat{R}_1))$. Here, $D_5 = C_{\hat{R}_7}(\hat{R}_1) \bmod \acute{n}$, $D_2 = C_{\hat{R}_6}(\mathcal{P}_{TA}) \bmod \acute{n}$, $A_1 = ID_{OP} \oplus P_{SN}$ and $MT_{S2} = C_{\hat{R}_2}(\mathcal{P}_{TA}) \bmod \acute{n}$. To derive $C_{\hat{R}_6}(C_{\hat{R}_7}(\hat{R}_1))$ from D_1 and D_5 is equivalent solving the chaotic-maps-based Diffie–Hellman problem or chaotic-maps-based discrete logarithm problem. Since this is computationally infeasible, adversary Å is unable to derive the generated session key. □

Hypothesis 6. *The proposed scheme is resilient against packet replay and MITM attacks.*

Proof. In the proposed scheme, we deploy nonces $\hat{R}_6$ and $\hat{R}_7$ in each session as elaborated upon in Hypothesis 5. Based on Hypothesis 3, the MT, TA and GWN execute strong mutual authentication before commencing packet exchanges. As such, adversary Å is unable to masquerade as the legitimate MT, GWN or TA so as to mount MITM attacks. □

Hypothesis 7. *The proposed scheme upholds MT anonymity.*

Proof. In the proposed scheme, the MT identity ID_{OP} is masked in A_1, where $A_1 = ID_{OP} \oplus P_{SN}$. On the other hand, ID_{OP} is hashed in A_4, A_5 and $\hat{R}_3$, where $A_4 = \hat{R}_3 \oplus h_2(ID_{OP}, SC_{OP}, x_1)$, $A_5 = h_2(ID_{OP}, A_2)$ and $\hat{R}_3 = A_4 \oplus h_2(ID_{OP}, SC_{OP}, x_1)$. Since A_1 is never transmitted over the communication channels, adversary Å cannot capture it. On the other hand, the attacker needs to reverse the one-way hashing functions A_4, A_5 and $\hat{R}_3$ to obtain this identity. Since this is computationally infeasible, the anonymity of the operator is upheld. □

4.2. Performance Analysis

In this sub-section, the cryptographic execution time, communication costs and resilience to attacks are used as the main metrics in the appraisal of the proposed scheme.

4.2.1. Execution Time

In this analysis, consideration is given to the cryptographic operations that are executed only during the mutual authentication and key agreement phase. During this phase, the fuzzy extraction T_F, elliptic curve point multiplication T_E, one-way hashing T_H and Chebyshev map T_C operations are executed. Based on the values in [46], $T_E = 63.08$ ms, $T_C = 21.02$ ms, $T_F = 63.08$ ms and $T_H = 0.5$ ms, as shown in Table 2.

For other related schemes, symmetric encryption and decryption T_{ED}, the Chinese remainder theorem (CRT) T_{CR} and elliptic curve modular exponential T_{EE} operations are required. Based on [46], $T_{ED} = 8.70$ ms, the execution time for $T_{CR} = 11$ ms and for $T_{EE} = 30$ ms. During the mutual authentication and key agreement phase, the $1T_F$, $6T_C$ and

23 T_H operations are executed. Table 3 gives the derivation of the execution times for the proposed scheme as well as other related schemes.

Table 2. Cryptographic runtimes.

Operation	Symbol	Runtime (ms)
Fuzzy extraction	T_F	63.08
EC point multiplication	T_E	63.08
Symmetric encryption/decryption	T_{ED}	8.70
One-way hashing	T_H	0.5
Chebyshev chaotic map	T_C	21.02
EC modular exponential	T_{EE}	30
CRT	T_{CR}	11

Table 3. Execution time comparison.

Scheme	Operations	Runtime (ms)
Abbasinezhad-Mood et al. [20]	$10T_C + 1T_{ED} + 40T_H$	238.9
Li et al. [34]	$1T_F + 6T_E + 22T_H$	452.56
Srinivas et al. [21]	$1T_{EE} + 1T_{CR} + 37T_H$	59.5
Wang et al. [22]	$1T_F + 6T_C + 22T_H$	200.2
Proposed	$1T_F + 6T_C + 23T_H$	200.7

As shown in Table 3, the protocol in [34] has the highest runtime of 452.56 ms followed by the schemes in [20] with a runtime of 238.9 ms. On the other hand, the proposed scheme has the third highest execution time of 200.7 ms, while the protocol in [22] has the second lowest execution time of 200.2 ms. On the other hand, the scheme in [21] has the lowest runtime of only 59.5 ms.

Although the protocol in [21] has excellent execution time, it cannot withstand side-channeling attacks through power analysis and cannot offer both perfect backward and forward key secrecy. In addition, this scheme has extremely high communication costs. On the other hand, the scheme in [22] cannot withstand side-channeling attacks and has very high communication costs. As such, although the proposed scheme has a slightly high execution time, it offers most of the security features required in wireless networks.

4.2.2. Communication Costs

In this analysis, the size of the exchanged messages during mutual authentication and key agreement are taken into consideration. Here, the outputs of nonces, ECC, symmetric encryption and decryption, integer factorization cryptography, hashing, timestamp and Chebyshev chaotic map are 128 bits, 256 bits, 128 bits, 3072 bits, 128 bits, 32 bits and 128 bits, respectively, as shown in Table 4.

Table 4. Message sizes.

Operation	Size (Bits)
Nonce	128
ECC	256
Symmetric encryption/decryption	128
One-way hashing	128
Chebyshev chaotic map	128
Timestamp	32
Integer factorization cryptography	3072

During the mutual authentication and key agreement phase, the following four messages are exchanged: $\{D_1, D_4, D_3\}$, $\{MAC_T, E_1, D_1\}$, $\{D_5, E_3, MAC_G\}$ and MAC_{New}. The sizes of these messages are computed as follows:

$$MAuth_{Req}: \{D_1 = D_4 = D_3 = 128\} = 384 \text{ bits}$$

$$GAuth_{Req}: \{MAC_T = E_1 = D_1 = 128\} = 384 \text{ bits}$$

$$GAuth_{Res}: \{D_5 = E_3 = MAC_G = 128\} = 384 \text{ bits}$$

$$MAuth_{Res}: MAC_{New} = 128 \text{ bits}$$

Based on the computations above, the total size of the four exchanged messages is 1280 bits. On the other hand, the schemes in [20–22,34] are 2048 bits, 3200 bits, 4448 bits and 1664 bits, respectively. Table 5 presents the derivation of these message sizes for the various schemes.

Table 5. Communication Costs Comparison.

	Abbasinezhad-Mood et al. [20]	Li et al. [34]	Srinivas et al. [21]	Wang et al. [22]	Proposed
M_1	768	896	3360	544	384
M_2	512	768	544	416	384
M_3	512	768	544	416	384
M_4	256	768	-	288	128
Total	2048	3200	4448	1664	1280

As shown in Table 5, the protocol in [21] has the highest communication costs of 4448 bits, followed by the protocol in [34] with communication costs of 3200 bits. The scheme in [20] has the third highest communication costs of 2048 bits, while the protocol in [22] has the highest communication costs of 1664 bits.

On the other hand, the proposed scheme has the lowest communication costs of 1280 bits. Consequently, the proposed scheme is the most ideal for sensor nodes which are limited in terms of computation, energy, memory and communication capabilities.

4.2.3. Attacks Resilience

To show that the proposed scheme offers resilience against most of the typical attacks in wireless networks, its security and privacy features are compared against those provided by the protocols in [20–22,34]. Table 6 presents this comparison using backward and forward key secrecy, secret ephemeral leakage, mutual authentication, side-channeling, session key agreement, packet replay, MITM and anonymity as key metrics.

Table 6. Security features comparison.

	Abbasinezhad-Mood et al. [20]	Li et al. [34]	Srinivas et al. [21]	Wang et al. [22]	Proposed
Backward and forward key secrecy	Y	Y	N	Y	Y
Secret ephemeral leakage	Y	N	Y	Y	Y
Mutual authentication	Y	Y	Y	Y	Y
Side channeling	N	Y	N	N	Y
Session key agreement	Y	Y	Y	Y	Y
Packet replay	Y	Y	Y	Y	Y
MITM	Y	Y	Y	Y	Y
Anonymity	Y	Y	Y	Y	Y
	Key Y = Security feature supported N = Security feature not supported				

Based on the results in Table 6, the scheme in [21] supports the least security and privacy features, followed by the schemes in [20,22,34], which lack one security feature. On the other hand, the proposed scheme offers support for all the security and privacy features. As such, it offers robust integrity protection in wireless networks.

4.2.4. Complexity Level Comparisons

In the performance evaluation of network security protocols, computation and communication complexities are frequently utilized. Here, the computation complexities indicate the duration it takes for various cryptographic operations to be executed. On the other hand, communication complexity denotes the number or length of the messages exchanged in these protocols. In this paper, computation complexity is measured using the execution time, while communication complexity is measured using the communication costs. These complexities are then compared with those obtained in other related schemes developed in [20–22,34].

In terms of computation complexity, it has been shown that the proposed scheme incurs the third highest execution time of 200.7 ms. However, the proposed scheme incurs the lowest communication complexity of only 1280 bits. On the other hand, the scheme developed in [34] has the highest computation complexity of 452.56 ms. Similarly, the scheme presented in [21] has the highest communication complexity of 4448 bits. Among the related schemes, the one developed in [22] has the lowest communication complexity of 1664 bits. As such, the proposed protocol offers a 23.08% improvement in the communication complexity.

5. Conclusions

The literature reviewed has pointed to the existence of many security schemes for the protection of the information exchanged over wireless sensor networks. It has been observed that these protocols are based on techniques such as machine learning, bilinear pairing operations, elliptic curve cryptography, chaotic maps, biometrics and smart cards, among other methods. However, it has been shown that long authentication latencies and execution times, as well as high communication overheads, are major performance issues in these protocols. Although these schemes improve some aspects of WSN security and privacy, the majority of them have been shown to be weak against common attacks in typical wireless networks. To address these issues, the developed scheme incorporates biometrics and extended Chebyshev chaotic maps during the authentication and key agreement process. Thus, the proposed scheme has the lowest execution time of 200.7 milliseconds and the highest security aspect compared to the related methods. In detail, the results show that this effectively renders the developed scheme resilient against numerous attacks such as packet replays, side-channeling and entity impersonations. In terms of performance evaluation, the deployed cryptographic operations are relatively lightweight and hence the execution time as well as the communication overheads of the proposed protocol are relatively low. Compared with other related schemes, the proposed protocol offers the best security features at the lowest communication overheads and a relatively low execution time. Future work could push towards decentralization in authentication, access and authorization. This may facilitate distributed and decentralized security provisioning that could enable direct integration into client end-point devices.

Author Contributions: Z.A.A. and V.O.N.; methodology, and writing—original draft preparation, M.J.J.G.; software, and data curation, I.Q.A.; validation, and writing—review and editing, M.A.A.S. and J.M.; formal analysis, investigation, supervision, project administration, and funding acquisition, A.J.Y.A.; resources, and visualization. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by university-enterprise cooperative R&D project of SZTU (grant no.20221061030001).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: All individuals included in this section have consented to the acknowledgement.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kumar, D.; Singh, H.K.; Ahlawat, C. A secure three-factor authentication scheme for wireless sensor networks using ECC. *J. Discret. Math. Sci. Cryptogr.* **2020**, *23*, 879–900. [CrossRef]
2. Peter, S.N.; Nyangaresi, V.O.; Ogara, S.O. Efficient Authentication Algorithm for Secure Remote Access in Wireless Sensor Networks. *J. Comput. Sci. Res.* **2021**, *3*, 43–50.
3. Rashid, B.; Rehmani, M.H. Applications of wireless sensor networks for urban areas: A survey. *J. Netw. Comput. Appl.* **2016**, *60*, 192–219. [CrossRef]
4. Karakaya, A.; Akleylek, S. A survey on security threats and authentication approaches in wireless sensor networks. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; pp. 1–4.
5. Wu, F.; Li, X.; Xu, L.; Vijayakumar, P.; Kumar, N. A novel three-factor authentication protocol for wireless sensor networks with IoT notion. *IEEE Syst. J.* **2020**, *15*, 1120–1129. [CrossRef]
6. Nyangaresi, V.O. ECC Based Authentication Scheme for Smart Homes. In Proceedings of the 2021 International Symposium ELMAR, Zadar, Croatia, 13–15 September 2021; pp. 5–10.
7. Liu, X.; Li, W.; Han, F.; Xie, Y. An optimization scheme of enhanced adaptive dynamic energy consumption based on joint network-channel coding in wsns. *IEEE Sens. J.* **2017**, *17*, 6119–6128. [CrossRef]
8. Ali, R.; Pal, A.K.; Kumari, S.; Karuppiah, M.; Conti, M. A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. *Future Gener. Comput. Syst.* **2018**, *84*, 200–215. [CrossRef]
9. Miranda, C.; Kaddoum, G.; Bou-Harb, E.; Garg, S.; Kaur, K. A collaborative security framework for software-defined wireless sensor networks. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2602–2615. [CrossRef]
10. Nyangaresi, V.O.; Ogundoyin, S.O. Certificate Based Authentication Scheme for Smart Homes. In Proceedings of the 2021 3rd Global Power, Energy and Communication Conference (GPECOM), Antalya, Turkey, 5–8 October 2021; pp. 202–207.
11. Nyangaresi, V.O.; Rodrigues, A.J.; Abeka, S.O. Efficient Group Authentication Protocol for Secure 5G Enabled Vehicular Communications. In Proceedings of the 2020 16th International Computer Engineering Conference (ICENCO), Cairo, Egypt, 29–30 December 2020; pp. 25–30.
12. Nyangaresi, V.O. Hardware Assisted Protocol for Attacks Prevention in Ad Hoc Networks. In Proceedings of the International Conference for Emerging Technologies in Computing, London, UK, 19–20 August 2021; Springer: Cham, Switzerland; pp. 3–20.
13. Shin, S.; Kwon, T. A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated Internet of Things. *IEEE Access* **2020**, *8*, 67555–67571. [CrossRef]
14. He, D.; Kumar, N.; Chen, J.; Lee, C.C.; Chilamkurti, N.; Yeo, S.S. Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. *Multimed. Syst.* **2015**, *21*, 49–60. [CrossRef]
15. Li, X.; Niu, J.; Kumari, S.; Liao, J.; Liang, W.; Khan, M.K. A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. *Secur. Commun. Netw.* **2016**, *9*, 2643–2655. [CrossRef]
16. Wu, F.; Xu, L.; Kumari, S.; Li, X. An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. *Multimed. Syst.* **2017**, *23*, 195–205. [CrossRef]
17. Ostad-Sharif, A.; Arshad, H.; Nikooghadam, M.; Abbasinezhad-Mood, D. Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme. *Future Gener. Comput. Syst.* **2019**, *100*, 882–892. [CrossRef]
18. Chen, Y.; Ge, Y.; Wang, Y.; Zeng, Z. An improved three-factor user authentication and key agreement scheme for wireless medical sensor networks. *IEEE Access* **2019**, *7*, 85440–85451. [CrossRef]
19. Adavoudi-Jolfaei, A.; Ash-Talouki, M.; Aghili, S.F. Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks. *Peer-Peer Netw. Appl.* **2019**, *12*, 43–59. [CrossRef]
20. Abbasinezhad-Mood, D.; Nikooghadam, M. Efficient Anonymous Password-Authenticated Key Exchange Protocol to Read Isolated Smart Meters by Utilization of Extended Chebyshev Chaotic Maps. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4815–4828. [CrossRef]
21. Srinivas, J.; Das, A.K.; Kumar, N.; Rodrigues, J.J. Cloud Centric Authentication for Wearable Healthcare Monitoring System. *IEEE Trans. Dependable Secur. Comput.* **2018**, *17*, 942–956. [CrossRef]
22. Wang, F.; Xu, G.; Xu, G. A Provably Secure Anonymous Biometrics- Based Authentication Scheme for Wireless Sensor Networks Using Chaotic Map. *IEEE Access* **2019**, *7*, 101596–101608. [CrossRef]
23. Jiang, Q.; Ma, J.; Lu, X.; Tian, Y. An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks. *Peer-to-Peer Netw. Appl.* **2015**, *8*, 1070–1081. [CrossRef]
24. Wu, F.; Xu, L.; Kumari, S.; Li, X. A new and secure authentication scheme for wireless sensor networks with formal proof. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 16–30. [CrossRef]

25. Park, Y. Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks. *Sensors* **2016**, *16*, 2123. [CrossRef]
26. Wang, C.; Xu, G.; Sun, J. An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks. *Sensors* **2017**, *17*, 2946. [CrossRef] [PubMed]
27. Maurya, A.; Sastry, V.N. Fuzzy extractor and elliptic curve based efficient user authentication protocol for wireless sensor networks and Internet of Things. *Information* **2017**, *8*, 136. [CrossRef]
28. Das, A.K. A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor. *Int. J. Commun. Syst.* **2017**, *30*, e2933. [CrossRef]
29. Das, A.K. A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks. *Peer–Peer Netw. Appl.* **2016**, *9*, 223–244. [CrossRef]
30. Das Kumar, A. A secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed wireless sensor networks. *Wirel. Pers. Commun.* **2015**, *82*, 1377–1404.
31. Wu, F.; Xu, L.; Kumari, S.; Li, X. An improved and provably secure three-factor user authentication scheme for wireless sensor networks. *Peer–Peer Netw. Appl.* **2016**, *11*, 1–20. [CrossRef]
32. Amin, R.; Islam, S.H.; Biswas, G.; Khan, M.K.; Leng, L.; Kumar, N. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Comput. Netw.* **2016**, *101*, 42–62. [CrossRef]
33. Jiang, Q.; Zeadally, S.; Ma, J.; He, D. Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. *IEEE Access* **2017**, *5*, 3376–3392. [CrossRef]
34. Li, X.; Niu, J.; Bhuiyan, M.Z.A.; Wu, F.; Karuppiah, M.; Kumari, S. A Robust ECC-Based Provable Secure Authentication Protocol with Privacy Preserving for Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3599–3609. [CrossRef]
35. Amjad, M.; Qureshi, H.K.; Lestas, M.; Mumtaz, S.; Rodrigues, J.J.P.C. Energy prediction based MAC layer optimization for harvesting enabled WSNs in smart cities. In Proceedings of the 87th IEEE Vehicular Technology Conference, Porto, Portugal, 3–6 June 2018; pp. 1–6.
36. Murugesan, R.; Saravanan, M.; Vijyaraj, M. A node authentication clustering based security for adhoc network. In Proceedings of the 2014 6th International Symposium on Communications, Control and Signal Processing (ISCCSP), online, 21–23 May 2014; pp. 1168–1172.
37. Zhu, C.; Leung, V.C.; Yang, L.T.; Shu, L. Collaborative location based sleep scheduling for wireless sensor networks integrated with mobile cloud computing. *IEEE Trans. Comput.* **2015**, *64*, 1844–1856. [CrossRef]
38. Yin, C.; Zhu, Y.; Fei, J.; He, X. A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access* **2017**, *5*, 21954–21961. [CrossRef]
39. Ma, T.; Yu, Y.; Wang, F.; Zhang, Q.; Chen, X. A hybrid methodologies for intrusion detection based deep neural network with support vector machine and clustering technique. *Sensors* **2016**, *16*, 1701. [CrossRef] [PubMed]
40. Ambusaidi, M.A.; He, X.; Nanda, P.; Tan, Z. Building an intrusion detection system using a filter-based feature selection algorithm. *IEEE Trans. Comput.* **2016**, *65*, 2986–2998. [CrossRef]
41. Kim, J.; Kim, J.; Thu, H.L.T.; Kim, H. Long short term memory recurrent neural network classifier for intrusion detection. In Proceedings of the IEEE 2016 International Conference on Platform Technology and Service (PlatCon), Jeju, South Korea, 15–17 February 2016; pp. 1–5.
42. Li, F.; Xiong, P. Practical secure communication for integrating wireless sensor networks into the internet of things. *IEEE Sens. J.* **2013**, *13*, 36773684. [CrossRef]
43. Nyangaresi, V.O. Lightweight Key Agreement and Authentication Protocol for Smart Homes. In Proceedings of the 2021 IEEE AFRICON, Arusha, Tanzania, 13–15 September 2021; pp. 1–6.
44. Chen CL, Shih TF, Tsai YT, Li DK. A bilinear pairing-based dynamic key management and authentication for wireless sensor networks. *J. Sens.* **2015**, *2015*, 1–15.
45. Nyangaresi, V.O.; Rodrigues, A.J.; Taha, N.K. Mutual Authentication Protocol for Secure VANET Data Exchanges. In Proceedings of the International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures, Virtula Event, 6–7 May 2021; Springer: Cham, Switzerland; pp. 58–76.
46. Roy, S.; Chatterjee, S.; Das, A.K.; Chattopadhyay, S.; Kumari, S.; Jo, M. Chaotic Map-Based Anonymous User Authentication Scheme with User Biometrics and Fuzzy Extractor for Crowds the proposed cing Internet of Things. *IEEE Internet Things J.* **2018**, *5*, 2884–2895. [CrossRef]

View publication stats