Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things

Mustafa A. Al Sibahee[1,2], Vincent Omollo Nyangaresi[3], Junchao Ma[1(✉)], and Zaid Ameen Abduljabbar[4,5]

[1] College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
{mustafa,majunchao}@sztu.edu.cn
[2] Computer Technology Engineering Department, Iraq University College, Basrah, Iraq
mustafa.alsibahee@iuc.edu.iq
[3] Faculty of Biological and Physical Sciences, Tom Mboya University College, Homabay, Kenya
vnyangaresi@tmuc.ac.ke
[4] Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq
zaid.ameen@uobasrah.edu.iq
[5] Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen, China

Abstract. To ensure secure access to the data held in internet of things, many lightweight authentication schemes have been developed using approaches such as symmetric cryptography or hashing operations. Although these schemes achieve forward key secrecy and user anonymity, de-synchronization is a major problem in these protocols. As such, many other schemes have been presented to address this pertinent security challenge. However, some of these schemes are still susceptible to smart card loss attacks among others. In this paper, stochastic security ephemeral generation protocol for 5G enabled internet of things is presented. It is demonstrated to offer mutual authentication and session key agreement. It is also robust against packet replays, eavesdropping and man-in-the-middle attacks. In terms of performance, it has the lowest computation and communication overheads.

Keywords: 5G · Authentication · Ephemeral · IoT · Key agreement · Stochastic

1 Introduction

The Internet of Things (IoT) is a fairly recent technology that executes remote sensing and control in heterogeneous networks. To achieve this, Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSNs) are deployed [1]. It basically consists of sensors, home appliances and smart devices such as smart-phones that users deploy to interact with the controlled devices [2]. In this scenario, the home appliances owners exchange packets with the controlled devices over the internet. According to [3], WSNs play critical roles in industrial internet of things (IIoT). As explained in [1], the incorporation of cloud computing with IoT can realize various smart environments such as smart

W. Hussain and M. A. Jan (Eds.): IoTaaS 2021, LNICST 421, pp. 3–18, 2022.
https://doi.org/10.1007/978-3-030-95987-6_1

transport system, smart healthcare and smart grid [4]. Here, the smartness crops from the usage of smart sensors to perceive and collect information from the environment.

According to [5], the WSN is composed of miniature low powered sensors that act as nodes and have found applications in agriculture, military, disaster management, surveillance systems, environmental monitoring and safety. As explained in [6], the sensors perceive their environment and transmit the collected data to the base stations (sink nodes). Unfortunately, these sensor nodes are resource limited in terms of computation power and storage [7, 8]. In addition, WSN have coverage, energy, security and connectivity constraints [9]. Due to its support for device ultra-densification and high bandwidths, 5G networks form the backbone for most of the IoT applications such as smart homes [10], smart cities [11], smart health and smart grids [12].

Despite the many application domains of IoT and the attained convenience, industrial WSN (IWSN) face numerous privacy and security challenges owing to their internet connectivity from unattended environments [9]. The need to access real-time data from the sensor nodes calls for strong user authentication protocols. Since smart-phones are increasing being used to access and control IoT devices [2] over cellular networks or Wi-Fi networks, there is need to protect malware in these devices. According to [13], the usage of broadcast messages in WSN can lead to various attacks and vulnerabilities. As such, there is need for sensor nodes to execute authentication and key agreement before accepting packets from each other. Authors in [14] explain that IoT sensors collect private and sensitive data such as personal health information emanating from wearable medical devices. In addition, home sensors and vehicular ad hoc networks (VANETs) also collect and transmit private data that must be properly protected.

Authors in [5] have identified smart card loss, offline guessing, sensor node capture as being serious challenges in WSN, due to the open wireless transmission medium and operation in unattended environment. Consequently, the provision of privacy and security in WSN is a challenging task. The results of any data leakages or successful attack in WSNs are catastrophic due to their sensitivity, for instance in the military [13]. There is therefore need for secure transmission of the exchanged packets to the end devices. Authors in [15] have identified the openness of the deployed communication medium as being a major challenge in WSN. Proper authentication between the user and the sensor node has therefore been recommended. On the other hand, the integration of 5G and IoT has been identified in [16] as having increased the attack surfaces in an IoT environment.

As explained in [17], the resource limitation of sensor nodes, coupled with the transfer of data over open wireless channels render security the biggest challenge during deployment of WSNs. Since users can access the sensor node data anytime and from any location, authentication is key before this access is granted. On the other hand, authors in [7] have identified bogus message insertion, packet interception, malicious deletion and packet re-routing as being major issues in WSNs. Similarly, active and passive attacks have been identified in [18] as being critical challenges. In addition, authors in [9] have cited physical and cloning attacks as serious threats in IWSNs. Enforcing session key agreement and user authentication is tricky due to the difficulty in replacing or recharging battery of deployed sensors [7]. As such, reduction of energy consumption at the sensor node is crucial. Unfortunately, the conventional internet protocols are inapplicable in

IoT due to the low computation power of the supported devices [5]. Consequently, the design of efficient security protocols for IoT devices is still challenging due to their resource constrained nature [3].

To boost privacy in these networks, anonymity and untraceability need to be implemented [19]. Here, anonymity hides participants' identity so that there is no knowledge of who accesses data at particular instant. On the other hand, untraceability prevents tracking of particular user's different sessions based on the exchanged packets. In addition, authorization and access control are essential in securing IoT messages.

Based on the above mentioned challenges, secure communication is vital for the protection of packets exchanged over IoT environment. To achieve this, user authentication should be executed, followed by key agreement [20, 21]. As such, many lightweight authentication and key agreement protocols have been designed based on symmetric encryption and decryption algorithms. However, most of these schemes still face desynchronization threats as they pursue forward key secrecy and anonymity [22]. Consequently, upholding secure access to private and sensitive data in an IoT environment is still an open challenge, owing to the large attack vectors [7]. The major contributions of this paper include the following:

- A trusted authority based authentication scheme is developed to offer stochastic generation of security tokens needed for secure packet exchanges in an IoT environment.
- Message source authentication is executed to protect against session hijacking and de-synchronization attacks.
- Security analysis is carried out to demonstrate that the proposed protocol offers key agreement and mutual authentication, in addition to thwarting attacks such as man-in-the-middle.
- The performance of the proposed protocol, is executed using communication and computation costs as metrics, which shows that the proposed protocol has the least values of these two metrics.

The rest of this research paper is organized as follows: Sect. 2 presents related work in this research domain while Sect. 3 discusses the system model of the proposed protocol. On the other hand, Sect. 4 presents and discusses comparative evaluation of the proposed protocol while Sect. 5 concludes the paper and offers some future directions.

2 Related Work

Security and privacy challenges in IoT devices have seen the development of a myriad of authentication protocols. However, none of these schemes effectively satisfies IoT security issues at low performance costs. For instance, an authentication and key agreement (AKA) protocol presented in [23] has a number of security flaws [24, 25]. On the other hand, the schemes in [26, 27] cannot uphold forward key secrecy and user anonymity [28]. Similarly, the protocol in [29] has some security vulnerabilities [30]. Although the scheme in [31] upholds authentication, confidentiality, integrity and non-repudiation, the deployed bilinear pairing operations lead to high computational complexities [32].

Authors in [33] introduce a temporal key based user authentication scheme that is shown to have high efficiency. However, this approach is susceptible to impersonation, offline guessing and injection attacks [34].

A novel three-factor authentication approach is developed in [35], but authors in [36] point out that this scheme has security flaws. Similarly, a bio-hashing protocol is presented in [37], but which is vulnerable to privileged insider and node capture attacks. In addition, this scheme fails to offer user anonymity [27]. On the other hand, the scheme in [38] offers protection against traceability, offline-guessing, impersonation, packet replays and side-channel attacks, but at the expense of slightly high communication and computation overheads. Although the protocol in [34] addresses some of the security weakness of the scheme in [33], it is susceptible to traceability, impersonation and smart card loss attacks. Similarly, the two-factor authentication scheme in [39] is not robust against some attacks [30]. The biometrics-based scheme in [40] is vulnerable to collusion and de-synchronization attacks, and cannot offer sensor node anonymity [39]. On the other hand, the elliptic curve cryptography (ECC) based technique in [41], just like the schemes in [33, 34], is susceptible to de-synchronization and ephemeral leakage attacks.

The protocol presented in [28] is unable to detect invalid passwords during logins while the scheme in [42] is susceptible to de-synchronization and physical capture attacks [40], and does not offer sensor node anonymity [22]. Similarly, the protocol in [43] is vulnerable to smart card loss, offline password guessing and traceability attacks. In addition, the biometric authentication scheme in [2] is susceptible to smart card loss attacks. On the other hand, the two-factor protocol in [44] is vulnerable to session key disclosure, impersonation and smart card loss attacks [45]. Similarly, the fuzzy verifier based scheme in [46] is susceptible to replay attacks. Although the protocol in [47] can prevent de-synchronization attacks, it has high communication and computation overheads.

The anonymous three-factor authentication scheme in [24] prevents offline guessing attacks, but is susceptible to privileged insider attacks. On the other hand, the protocol in [45] is vulnerable to offline password guessing, smart card loss and impersonation attacks [35]. Although the authors in [48] claim that their scheme prevents known attacks, this scheme is not robust against known secret attacks and has high computation costs. On the other hand, the scheme in [49] is vulnerable to forgery and offline password guessing attacks [28].

3 System Model

The entities involved in the proposed protocol include the sensor device (SD), trusted authority (TA) and the gateway node (GWN) as shown in Fig. 1. In this network model, the sensor node gathers relevant data upon request by its operators.

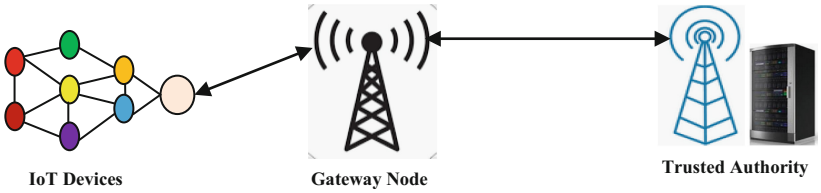

Fig. 1. Network model

It then processes the collected data before transmitting it to the target entity such as a GWN. Table 1 presents the symbols used in this paper, including their brief descriptions.

Table 1. Symbols and their descriptions

Symbol	Description
SID_i	Smart device identity
$\breve{g}$	TA secret key
$E_{\breve{K}}$	Encryption using key $\breve{K}$
$D_{\breve{K}}$	Decryption using key $\breve{K}$
U_{ID}	User identity
β	User secret key
$\check{Z}$	User's authentication token
T_e	Expiration time for $\check{Z}$
T_i	Timestamp
ID_{GWN}	Gateway node identity
β^*	Session key
$\mathbb{N}_i$	Random nonce

The proposed protocol then executes system parameter setting, which is followed by mutual authentication and key agreement. These two major phases are discussed below.

3.1 System Parameter Setting Phase

The activities carried out during this phase involves the generation of security parameters by the TA, which are then assigned to both the gateway node and the sensor device as explained in steps 1 to 4.

Step 1: The trusted authority (TA) derives secret key pair (A_i, B_i) for each IoT sensor device SD_i, which is then buffered in its memory before being transmitted to these devices through some secure channels.

Step 2: Each SDi generates random challenge C_i at timestamp T_i before storing them in its tamper proof device (TPD). This is followed by the TPD's computation of

$Ł_1 = h(A_i, SID_i, C_i, T_i)$. Next, SD_i composes $M_1 = \{Ł_1, SID_i, C_i, T_i\}$ and sends it together with registration request Reg_{Req} to the TA.

Step 3: On receipt of M_1, the TA executes integrity validation followed by data source authentication on the received message. To achieve this, it computes $Ł_1^* = h(A_i, SID_i, C_i, T_i)$ from its locally buffered A_i and the received $\{SID_i, C_i, T_i\}$. If $Ł_1^* \neq Ł_1$,, registration is aborted, otherwise the TA derives $Ł_2 = h(A_i, B_i + C_i)$. Next, it randomly selects secret key ğ before computing parameter $Ł_3 = h(ğ, SID_i, C_i)$. This is followed by the construction of registration response Reg_{Res} together with $M_2 = \{Ł_3, SID_i\}$ that is then conveyed to the SD_i through a secure channel.

Step 4: Upon receiving M_2, the SD_i derives $Ł_2^* = (A_i, B_i + C_i)$ at the TPD. Next, it calculates $Ł_3^* = h(ğ, SID_i, C_i)$ and checks whether $Ł_3^* = Ł_3$,. If this condition does not hold, M_2 is flagged as malicious, otherwise the SD_i trusts that M_2 was from a genuine TA.

3.2 Authentication and Key Agreement Phase

In this phase, the parameters that were assigned to the sensor nodes and gateway node during the previous phase are deployed to verify the messages exchanged among the communicating entities. After successful mutual authentication, a session key is derived to protect the exchanged packets as explained in step 1 to 6 below.

Step 1: The TA generates temporary key $Ķ_1 = h(ğ)$ followed by the derivation of security parameter $Ž = E_{Ķ_1}(U_{ID}, ƥ, T_e)$. It then forwards Ž to the user's SD_i, which stores it in its memory.

Step 2: The SD_i selects random number $\mathbb{N}_1$ and generates the message authentication code (MAC) $ϕ_{M1} = h(ƥ, U_{ID}, \mathbb{N}_1, Ž, T_1)$. Afterwards, the SD_i composes authentication request $Auth_{Req}$ together with $M_3 = \{U_{ID}, ID_{GWN}, \mathbb{N}_1, Ž, T_1, ϕ_{M1}\}$ that are then sent to the GWN.

Step 3: On receiving M_3, the GWN verifies whether the timestamp in this message is within the permitted range, and if this is not the case, the authentication request is rejected. However, if it is, the GWN derives temporary key $Ķ_1^* = h(ğ)$ that is utilized to decrypt the received Ž. This decryption yields security parameters ƥ and T_e. Next, the validity of T_e is confirmed such that if it is incorrect, the authentication session is terminated. However, if it is legitimate, the GWN utilizes the obtained ƥ to validate the received $ϕ_{M1}$. If $ϕ_{M1}$ is invalid, the GWN rejects the authentication request from the SD_i, otherwise it believes that $ϕ_{M1}$ is from a legitimate SD_i.

Step 4: The GWN selects random number $\mathbb{N}_2$ and computes message authentication code $ϕ_{M2} = h(ƥ, ID_{GWN}, \mathbb{N}_2, T_2)$. It then updates secret key $ƥ^* = h(ƥ, U_{ID}, ID_{GWN}, \mathbb{N}_2, \mathbb{N}_1)$. Finally, it composes authentication response $Auth_{Res}$ together with $M_4 = \{U_{ID}, ID_{GWN}, \mathbb{N}_2, T_2, ϕ_{M2}\}$ that are sent over to the SD_i.

Step 5: On receiving M_4, freshness check is executed on this message using timestamp T_2 such that if it is invalid, the authentication session is terminated. However, if it is valid, it proceeds to confirm whether $ϕ_{M2}$ is legitimate or not. On condition that the verification of T_2 and $ϕ_{M2}$ flops, the session is terminated, otherwise the SD_i computes secret key $ƥ^* = h(ƥ, U_{ID}, ID_{GWN}, \mathbb{N}_2, \mathbb{N}_1)$. Next, it derives $ϕ_{M3} = h(ƥ^*, U_{ID}, ID_{GWN}, \mathbb{N}_2, T_3)$ before composing $M_5 = \{ID_{GWN}, \mathbb{N}_2, T_3, ϕ_{M3}\}$ and delivering it to the GWN.

Step 6: After getting ϕ_{M3}, the GWN validates it such that if the verification is unsuccessful, the session is terminated, otherwise the GWN trusts the SD_i. Afterwards, the new secret key β^* is shared between the GWN and SD_i.

4 Comparative Analysis and Evaluation

In this section, the proposed protocol is evaluated using the various attack models as well as performance metrics as discussed in Sect. 4.1 and Sect. 4.2 below.

4.1 Security Evaluation

Both formal security analysis and informal analysis are carried out in this section to show the robustness of the proposed protocol. This is elaborated in Sects. 4.1.1 and Sect. 4.1.2 that follow.

Formal Security Analysis. In this section, the Burrows-Abadi-Needham (BAN) logic is employed as a formal model to proof that the proposed protocol attains the formulated security goals. To achieve this, the BAN logic rules and notations in [10, 19] are deployed. Based on the BAN logic analytical procedures, the following two goals are formulated:

Goal 1: $GWN|\equiv SD_i \overset{\beta}{\longleftrightarrow} GWN$

Goal 2: $GWN|\equiv SD_i \ |\equiv SD_i \overset{\beta^*}{\longleftrightarrow} GWN$

For the successful execution of the logical analysis of the proposed protocol, initial state assumptions (IAs) are critical. As such, the initial assumptions in Table 2 are made.

Table 2. Initial state assumptions

IA_1	$SD_i \ |\equiv SD_i \overset{\beta}{\longleftrightarrow} GWN$
IA_2	$SD_i \ |\equiv TA \overset{\breve{g}}{\longleftrightarrow} GWN$
IA_3	$GWN|\equiv TA \overset{\breve{g}}{\longleftrightarrow} GWN$
IA_4	$GWN|\equiv \#(T_e)$
IA_5	$GWN|\equiv (SD_i/TA)| \Rightarrow SD_i \overset{\beta}{\longleftrightarrow} GWN$
IA_6	$SD_i|\equiv \#(T_2)$
IA_7	$GWN|\equiv \#(T_1)$
IA_8	$GWN|\equiv \#(T_3)$
IA_9	$SD_i|\equiv \#(\mathbb{N}_1)$
IA_{10}	$GWN|\equiv \#(\mathbb{N}_2)$

During the mutual authentication and key agreement phase, messages $M_3 = \{U_{ID}, ID_{GWN}, \mathbb{N}_1, \check{Z}, T, \phi_{M1}\}$, $M_4 = \{U_{ID}, ID_{GWN}, \mathbb{N}_2, T_2, \phi_{M2}\}$ and $M_5 = \{ID_{GWN}, \mathbb{N}_2, T_3, \phi_{M3}\}$ are exchanged between the SD_i and GWN. For easier analysis during the BAN logic proofs, these three messages are transformed into idealized format as shown below.

$$\mathbf{M_3}\text{: } GWN \lhd \{U_{ID}, ID_{GWN}, \mathbb{N}_1, \check{Z}, T_1\{U_{ID}, SD_i \overset{ß}{\longleftrightarrow} GWN, T_3\}_{K_1},$$
$$\{U_{ID}, \mathbb{N}_1, T_1, \{U_{ID}, SD_i \overset{ß}{\longleftrightarrow} GWN, T_e\}_{K_1}\}_{ß}\}$$
$$\mathbf{M_4}\text{: } SD_i \lhd \{U_{ID}, ID_{GWN}, \mathbb{N}_2, T_2\{U_{GWN}, \mathbb{N}_2, T_2, SD_i \overset{ß^*}{\longleftrightarrow} GWN\}_{ß}$$
$$\mathbf{M_5}\text{: } GWN \lhd \{ID_{GWN}, \mathbb{N}_2, T_3, SD_i \overset{ß^*}{\longleftrightarrow} GWN\}_{ß^*}$$

Afterwards, based on the BAN logic rules, initial state assumptions and idealized message exchanges, the BAN logic proof proceeds as follows.

Based on M_3 and IA_3, the message meaning rule (MMR) is applied to yield B_1:

$\mathbf{B_1}$: $GWN \mid \equiv SD_i/TA|\sim\{U_{ID}, \mathbb{N}_1, T_1, ID_{GWN}, SD_i \overset{ß}{\longleftrightarrow} GWN, T_e\}$·

On the other hand, according to B_1, nonce verification rule (NVR) is applied in both IA_4 and IA_7 to obtain B_2:

$\mathbf{B_2}$: $GWN \mid \equiv SD_i| \equiv SD_i \overset{ß}{\longleftrightarrow} GWN$·

Based on B_2 and IA_5, jurisdiction rule (JR) is applied to get B_3:

$\mathbf{B_3}$: $GWN \mid \equiv SD_i \overset{ß}{\longleftrightarrow} GWN$, hence achieving **Goal 1**.·

According to M_4 and IA_1, the MMR is applied to obtain B_4:

$\mathbf{B_4}$: $SD_i \mid \equiv GWN|\sim \{ID_{GWN}, \mathbb{N}_2, T_2, SD_i \overset{ß}{\longleftrightarrow} GWN\}$·

On the other hand, based on B_4, IA_6 and IA_9 the application of NVR results in B_5:

$\mathbf{B_5}$: $SD_i| \equiv GWN \mid \equiv SD_i \overset{ß}{\longleftrightarrow} GWN$·

Afterwards, MMR is used in M_5 and B_3 to yield B_6:

$\mathbf{B_6}$: $GWN \mid \equiv SD_i|\sim\{ID_{GWN}, \mathbb{N}_2, T_3, SD_i \overset{ß^*}{\longleftrightarrow} GWN\}]$·

Based on IA_8, IA_{10} and B_6, the application of NVR results in B_7:

B_7: $GWN|\equiv SD_i \mid\equiv SD_i \overset{ß^*}{\longleftrightarrow} GWN$, attaining **Goal 2.**·

The attainment of both Goal 1 and Goal 2 demonstrates that the proposed protocol executes mutual authentication between the GWN and the SD_i before the onset of data exchanges between these two entities.

Informal Security Analysis. In this section, it is shown that the proposed protocol is resilient against some of the most common attack vectors in the internet of things environment. These attack vectors include man-in-the-middle, eavesdropping and packet replays. It is also shown that it offers mutual authentication and session key agreement.

Man-in-the-Middle Attacks. Suppose that an attacker is interested in deriving the new session key $ß^*$. To accomplish this, public parameters exchanged over the wireless channels must be eavesdropped. However, this new session key $ß^* = h(ß, U_{ID}, ID_{GWN}, \mathbb{N}_2, \mathbb{N}_1)$ is computed from secret values $ß$ after every successful mutual authentication. As such, without proper authentication to the GWN or SD_i, this attack is infeasible. Now, suppose that the attacker is interested in deriving valid MAC $\{\phi_{M1} = h(ß, U_{ID}, \mathbb{N}_1, \check{Z}, T_1)$, $\phi_{M2} = h(ß, ID_{GWN}, \mathbb{N}_2, T_2)$ and $\phi_{M3} = h(ß^*, U_{ID}, ID_{GWN}, \mathbb{N}_2, T_3)\}$ that may be utilized to fool the network entities. However, derivation of any valid MAC requires secret key $ß$ and hence MitM attack fails.

Mutual Authentication. The proposed protocol attains mutual authentication between the SD_i and GWN. Here, the GWN authenticates the SD_i by checking whether the received $\phi_{M1} = h(\beta, U_{ID}, \mathbb{N}_1, \check{Z}, T_1)$, where $\beta = D_{\check{K}_1}(\check{Z})$. Clearly, it is only legitimate SD_i that can derive secret key β needed to generate valid ϕ_{M1}. To authenticate the GWN, the SD_i confirms whether the received $\phi_{M2} = h(\beta, ID_{GWN}, \mathbb{N}_2, T_2)$. It is only the legitimate GWN that can derive $\check{K}_1 = h(\check{g})$ that is deployed to decrypt $\check{Z}$, thus obtaining secret key β. As such, there is a strong mutual authentication between SD_i and GWN.

Eavesdropping Attacks. In the proposed scheme, the GWN enciphers and encapsulates secret key β in $\check{Z} = E_{\check{K}_1}(U_{ID}, \beta, T_e)$ using ephemeral key $\check{K}_1 = h(\check{g})$. As such, even if an attacker intercepts authentication token $\check{Z}$ over the communication channel, secret key β cannot be derived since $\check{K}_1$ is unknown. In addition, the sensitive data protection encryption keys are never sent over the transmission channels. Consequently, adversaries cannot eavesdrop these keys and hence cannot access the sensitive messages being transmitted between the GWN and SD_i.

Session Key Agreement. In the proposed scheme, the SD_i negotiates some session key $\beta^* = h(\beta, U_{ID}, ID_{GWN}, \mathbb{N}_2, \mathbb{N}_1)$ with the GWN. This session key is derived from secret key β, and random numbers $\mathbb{N}_1$ and $\mathbb{N}_2$ that are dynamically derived by the SD_i and GWN respectively. Here, only the legitimate SD_i has knowledge of secret key β. Similarly, only the legitimate GWN can compute ephemeral $\check{K}_1 = h(\check{g})$ required to retrieve secret key β through the decryption of $\check{Z}$. The adversary is unable to derive the stochastic ephemeral keying parameters and hence cannot derive the established session key between the SD_i and GWN.

Packet Replay Attacks. Suppose that an attacker attempts to intercept the messages exchanged between the GWN and SD_i. Afterwards, bogus authetication message is constructed to fool the network entities. However, in the proposed protocol, timestamps are used to carry out the freshness checks of all received messages. Due to the limited permissible transmission delays, the intercepted and replayed message will have elongated transmission delay and hence will be easily detected at the end devices. Since these timestamps are hashed to obtain the message authentication codes $\phi_{M1} = h(\beta, U_{ID}, \mathbb{N}_1, \check{Z}, T_1)$, $\phi_{M2} = h(\beta, ID_{GWN}, \mathbb{N}_2, T_2)$ and $\phi_{M3} = h(\beta^*, U_{ID}, ID_{GWN}, \mathbb{N}_2, T_3)$, they cannot be modified and substituted with bogus ones. Consequently, the replayed packets are easily detected through verification of the message authentication codes, coupled with freshness checks. Table 3 presents the comparison of the security features provided by the proposed protocol and those of other related schemes.

It is evident that the proposed protocol has more security features compared with the rest of the schemes.

Table 3. Security features comparisons

Attack model	[29]	[39]	[48]	[28]	[38]	[24]	[3]	[46]	Proposed
Key agreement	√	√	√	√	√	√	√	√	√
Man-in-the-middle	√	√	√	√	-	√	x	√	√
Replay	x	x	√	x	√	√	x	x	√
Eavesdropping	-	-	-	-	-	-	-	-	√
Mutual authentication	√	√	√	√	√	√	√	√	√
	Legend √ Effective x Ineffective - Not considered								

4.2 Performance Evaluation

During the performance evaluation of authentication protocols, computation overheads as well as communication costs are the most utilized metrics. As such, in this section, it is shown that the proposed protocol has the lowest computation and communication costs when compared with other related approaches.

Computation Overheads. The proposed protocol executed a single one-way hashing (T_H) operation and one symmetric key encryption (T_E) during the system parameter setting phase. However, during the authentication and key agreement phase, $7T_H$, $1T_E$ and one symmetric decryption (T_D) operation are executed. Using the cryptographic execution times in [28] shown in Table 4, the computation overheads of the proposed protocol is derived.

Table 4. Cryptographic operations execution time

Cryptographic operation	Time (ms)
ECC point multiplication	7.3529
One-way hashing	0.0004
Symmetric encryption or decryption	0.1303
Bio-deterministic reproduction	7.3529

Based on the values in Table 4, the computation overhead of the proposed protocol is derived as follows:

$$7T_H\{7 * 0.0004 = 0.0028\}$$
$$1T_E\{1 * 0.1303 = 0.1303\}$$
$$1T_D\{1 * 0.1303 = 0.1303\}$$

As such, the total execution time of the proposed protocol during AKA procedures is 0.2634 ms. Table 5 presents the comparisons results of the obtained execution time with other related schemes.

Table 5. Computation overheads

Protocol	Overheads (ms)
[29]	29.94
[39]	29.42
[48]	51.99
[28]	36.77
[38]	1.04
[24]	51.48
[3]	29.42
[46]	44.13
Proposed	0.2634

Based on the values in Table 5, the scheme in [48] has the highest computation costs of 51.99 ms followed by the scheme in [24] with execution time of 51.48 ms. On the other hand, the proposed protocol has the least computation costs of 0.2634 ms. Consequently, it is the most applicable in an IoT environment where resources are limited in terms of computation power.

Communication Overheads. In this evaluation, a consideration is given to the size of the messages exchanged during the mutual authentication and key agreement phase. During this phase, messages $M_3 = \{U_{ID}, ID_{GWN}, \mathbb{N}_1, \check{Z}, T_1, \phi_{M1}\}$, $M_4 = \{U_{ID}, ID_{GWN}, \mathbb{N}_2, T_2, \phi_{M2}\}$ and $M_5 = \{ID_{GWN}, \mathbb{N}_2, T_3, \phi_{M3}\}$ are exchanged between the SD_i and GWN. Using the parameter sizes in Table 6, the communication overhead in the proposed protocol is derived.

Table 6. Parameter size

Parameter	Size (bits)
Identity	32
One-way hashing	160
Random nonce	128
AES symmetric encryption/decryption	128
Timestamp	32

Based on the values in Table 6, the communication overhead of the proposed protocol is computed as follows:

$$M_3 = \{U_{ID} = ID_{GWN} = T_1 = 32, \mathbb{N}_1 = \mathbb{Z} = 128, \Phi_{M1} = 160\} = 384 \text{ bits}$$
$$M_4 = \{U_{ID} = ID_{GWN} = T_2 = 32, \mathbb{N}_2 = 128, \Phi_{M2} = 160\} = 384 \text{ bits}$$
$$M_5 = \{ID_{GWN} = T_3 = 32, \mathbb{N}_2 = 128, \Phi_{M3} = 160\} = 352 \text{ bits}$$

As such, the cumulative communication overhead in the proposed protocol is 1120 bits, which is equivalent to 140 bytes. Table 7 presents the communication costs comparison results of the proposed protocol with other related schemes.

Table 7. Communication overheads

Protocol	Overheads (bits)
[29]	3208
[39]	3424
[48]	2880
[28]	3072
[38]	1920
[24]	2368
[3]	2496
[46]	2880
Proposed	1120

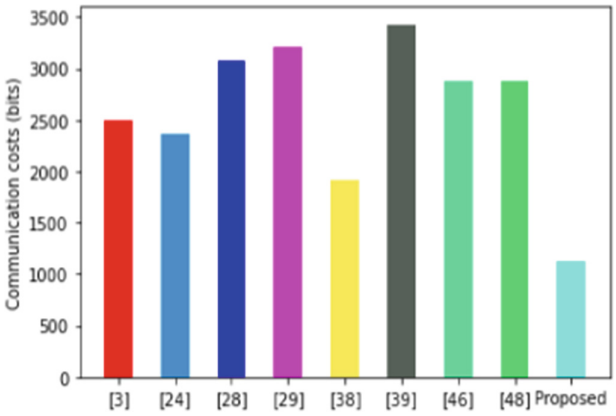

Fig. 2. Communication costs comparisons

Based on the values in Table 7, the graphs in Fig. 2 are plotted. It is clear from Fig. 2 that the protocol in [39] had the largest communication costs followed by the scheme in

[29]. On the other hand, the proposed protocol had the least number of bits exchanged during the authentication and key agreement phase. As such, the proposed protocol makes the most efficient usage of the network bandwidth. Consequently, it is ideal for deployment in an internet of things environment where devices are energy constrained. Since the number of bits transmitted is directly proportional to the energy consumed, the proposed protocol is the most energy efficient among all these other schemes.

Based on these analyses, the proposed scheme exhibits the lowest computation and communication overheads, and has most security features. As such, it has superior security features and best performance among all the other schemes.

5 Conclusion and Future Work

IoT devices have become ubiquitous to an extent that they potentially enhance convenience in people's day to day activities. These devices exchange massive amount of data that are private and sensitive. As such, any leakage of these data items can have devastating effects on the privacy of the parties involved in the communication process. Although many schemes have been developed to address these issues, they still face numerous security and performance issues. On the other hand, the presented protocol is shown to have the least communication and computation costs. As such, it is the most suitable for deployment in resource-constrained IoT devices. Moreover, the scheme offers admirable security features such as mutual authentication and key agreement, in addition to being resilient against a number of attacks such as packet replays. Future work in this research domain lies in the practical implementation of the proposed protocol in a real-world IoT scenario so that the attained performance and security issues can be verified.

Acknowledgements. This work is supported by Natural Science Foundation of Top Talent of SZTU (Grant number: 20211061010016).

References

1. Fu, Z., Huang, F., Ren, K., Weng, J., Wang, C.: Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data. IEEE Trans. Inf. Forensics Secur. **12**, 1874–1884 (2017)
2. 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 **8**, 67555–67571 (2020)
3. Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A.K., Choo, K.K.: A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. J. Netw. Comput. Appl. **103**, 194–204 (2018)
4. Nyangaresi, V.O., Affane Moundounga, A.R.: Secure data exchange scheme for smart grids. In: 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI), pp. 312–316. IEEE, Naples (2021)
5. Kumar, D., Singh, H.K., Ahlawat, C.: A secure three-factor authentication scheme for wireless sensor networks using ECC. J. Discrete Math. Sci. Cryptogr. **23**(4), 879–900 (2020)

6. Pundir, S., Wazid, M., Singh, D.P., Das, A.K., Rodrigues, J.J., Park, Y.: Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: survey and future challenges. IEEE Access **8**, 3343–3363 (2019)
7. Amin, R., Islam, S.H., Kumar, N., Choo, K.K.R.: An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks. J. Netw. Comput. Appl. **104**, 133–144 (2018)
8. Nyangaresi, V.O., Ogundoyin, S.O.: Certificate based authentication scheme for smart homes. In: 2021 3rd Global Power, Energy and Communication Conference (GPECOM), pp. 202–207. IEEE, Antalya (2021)
9. Gope, P., Das, A.K., Kumar, N., Cheng, Y.: Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks. IEEE Trans. Industr. Inf. **15**(9), 4957–4968 (2019)
10. Nyangaresi, V.O.: Lightweight key agreement and authentication protocol for smart homes. In: 2021 IEEE AFRICON, pp. 1–6. IEEE, Arusha (2021)
11. Zhu, H., Tan, Y.A., Zhu, L., Wang, X., Zhang, Q., Li, Y.: An identity-based anti-quantum privacy-preserving blind authentication in wireless sensor networks. Sensors **18**(5), 1–15 (2018)
12. Nyangaresi, V.O., Alsamhi, S.H.: Towards secure traffic signaling in smart grids. In: 2021 3rd Global Power, Energy and Communication Conference (GPECOM), pp. 196–201. IEEE, Antalya (2021)
13. Karakaya, A., Akleylek, S.: A survey on security threats and authentication approaches in wireless sensor networks. In: 2018 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1–4. IEEE, Antalya (2018)
14. Nyangaresi, V.: Hardware assisted protocol for attacks prevention in ad hoc networks. In: Miraz, M.H., Southall, G., Ali, M., Ware, A., Soomro, S. (eds.) iCETiC 2021. LNICSSITE, vol. 395, pp. 3–20. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-90016-8_1
15. Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J., Shu, L.: Authentication protocols for Internet of Things: a comprehensive survey. Secur. Commun. Network **2017**, 1–41 (2017)
16. Nyangaresi, V., Rodrigues, A., Taha, N.: Mutual authentication protocol for secure VANET data exchanges. In: Perakovic, D., Knapcikova, L. (eds.) FABULOUS 2021. LNICSSITE, vol. 382, pp. 58–76. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-78459-1_5
17. Shen, J., Chang, S., Shen, J., Liu, Q., Sun, X.: A lightweight multi-layer authentication protocol for wireless body area networks. Futur. Gener. Comput. Syst. **78**, 956–963 (2018)
18. Sureshkumar, C., Sabena, S.: Fuzzy-based secure authentication and clustering algorithm for improving the energy efficiency in wireless sensor networks. Wireless Pers. Commun. **112**(3), 1517–1536 (2020)
19. Nyangaresi, V.O., Petrovic, N.: Efficient PUF based authentication protocol for internet of drones. In: 2021 International Telecommunications Conference (ITC-Egypt), pp. 1–4. IEEE, Alexandria (2021)
20. Choo, K.K.R., Nam, J., Won, D.: A mechanical approach to derive identity-based protocols from Diffie-Hellman-based protocols. Inf. Sci. **281**, 182–200 (2014)
21. Nyangaresi, V.O., Mohammad, Z.: Privacy preservation protocol for smart grid networks. In: 2021 International Telecommunications Conference (ITC-Egypt), pp. 1–4. IEEE, Alexandria (2021)
22. Xiong, L., Xiong, N., Wang, C., Yu, X., Shuai, M.: An efficient lightweight authentication scheme with adaptive resilience of asynchronization attacks for wireless sensor networks. IEEE Trans. Syst. Man Cybern. Syst. **51**(9), 5626–5638 (2019)
23. Park, Y., Park, Y.: Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks. Sensors **16**(12), 2123 (2016)
24. Wang, C., Xu, G., Sun, J.: An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks. Sensors **17**(12), 2946 (2017)

25. Maurya, A., Sastry, V.N.: Fuzzy extractor and elliptic curve based efficient user authentication protocol for wireless sensor networks and Internet of Things. Information **8**(4), 136 (2017)
26. Das, A.K.: A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks. Peer-Peer Network. Appl. **9**(1), 223–244 (2016)
27. 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. **30**(1), e2933 (2017)
28. Wu, F., Xu, L., Kumari, S., Li, X.: An improved and provably secure three-factor user authentication scheme for wireless sensor networks. Peer-Peer Network. Appl. **11**(1), 1–20 (2018)
29. Wu, F., Xu, L., Kumari, S., Li, X.: A new and secure authentication scheme for wireless sensor networks with formal proof. Peer-Peer Network. Appl. **10**(1), 16–30 (2017)
30. Wang, D., Li, W., Wang, P.: Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Trans. Industr. Inf. **14**(9), 4081–4092 (2018)
31. Li, F., Xiong, P.: Practical secure communication for integrating wireless sensor networks into the internet of things. IEEE Sens. J. **13**(10), 3677–3684 (2013)
32. Nyangaresi, V.O., Rodrigues, A.J., Abeka, S.O.: Efficient group authentication protocol for secure 5G enabled vehicular communications. In: 2020 16th International Computer Engineering Conference (ICENCO), pp. 25–30. IEEE, Giza (2020)
33. Xue, K., Ma, C., Hong, P., Ding, R.: A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. J. Netw. Comput. Appl. **36**, 316–323 (2013)
34. He, D., Kumar, N., Chilamkurti, N.: A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. Inf. Sci. **321**, 263–277 (2015)
35. Amin, R., Islam, S.H., Biswas, G.P., Khan, M.K., Leng, L., Kumar, N.: Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. Comput. Netw. **101**, 42–62 (2016)
36. Jiang, Q., Zeadally, S., Ma, J., He, D.: Lightweight three-factor authentication and key agreement protocol for Internet-integrated wireless sensor networks. IEEE Access **5**, 3376–3392 (2017)
37. 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. Networks **9**(15), 2643–2655 (2016)
38. Peter, S.N., Vincent, O.N., Solomon, O.O.: Efficient authentication algorithm for secure remote access in wireless sensor networks. J. Comput. Sci. Res. **3**(4), 43–50 (2021)
39. Wu, F., Xu, L., Kumari, S., Li, X.: A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of things security. J. Ambient. Intell. Humaniz. Comput. **8**(1), 101–116 (2017)
40. Adavoudi-Jolfaei, A., Ashouri-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. **12**(1), 43–59 (2019)
41. Jiang, Q., Ma, J., Wei, F., Tian, Y., Shen, J., Yang, Y.: An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. J. Netw. Comput. Appl. **76**, 37–48 (2016)
42. Gope, P., Hwang, T.: A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. IEEE Trans. Ind. Electron. **63**(11), 7124–7132 (2016)
43. Chang, C.C., Le, H.D.: A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. IEEE Trans. Wireless Commun. **15**(1), 357–366 (2016)

44. Turkanović, M., Brumen, B., Hölbl, M.: A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. Ad Hoc Networks **20**, 96–112 (2014)
45. Farash, M.S., Turkanović, M., Kumari, S., Hölbl, M.: An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. Ad Hoc Networks **36**, 152–176 (2016)
46. Li, X., Peng, J., Obaidat, M.S., Wu, F., Khan, M.K., Chen, C.: A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. IEEE Syst. J. **14**(1), 39–50 (2019)
47. Xiong, L., Peng, D., Peng, T., Liang, H., Liu, Z.: A lightweight anonymous authentication protocol with perfect forward secrecy for wireless sensor networks. Sensors **17**(11), 2681 (2017)
48. Lu, Y., Xu, G., Li, L., Yang, Y.: Anonymous three-factor authenticated key agreement for wireless sensor networks. Wireless Netw. **25**(4), 1461–1475 (2019)
49. Das, A.K.: A secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed wireless sensor networks. Wireless Pers. Commun. **82**(3), 1377–1404 (2015)