BIG DATA MINING AND ANALYTICS
ISSN 2096-0654 01/07 pp1–9
Volume 4, Number 1, March 2021
DOI: 10.26599/BDMA.2020.9020010

New Enhanced Authentication Protocol for Internet of Things

Mourade Azrour*, Jamal Mabrouki, Azedine Guezzaz, and Yousef Farhaoui

Abstract: Internet of Things (IoT) refers to a new extended network that enables to any object to be linked to the Internet in order to exchange data and to be controlled remotely. Nowadays, due to its multiple advantages, the IoT is useful in many areas like environment, water monitoring, industry, public security, medicine, and so on. For covering all spaces and operating correctly, the IoT benefits from advantages of other recent technologies, like radio frequency identification, wireless sensor networks, big data, and mobile network. However, despite of the integration of various things in one network and the exchange of data among heterogeneous sources, the security of user's data is a central question. For this reason, the authentication of interconnected objects is received as an interested importance. In 2012, Ye et al. suggested a new authentication and key exchanging protocol for Internet of things devices. However, we have proved that their protocol cannot resist to various attacks. In this paper, we propose an enhanced authentication protocol for IoT. Furthermore, we present the comparative results between our proposed scheme and other related ones.

Key words: authetication; Internet of Things (IoT); sensor; security; authorization

1 Introduction

In recent digital world, the Internet of Things (IoT) is a great network technology that interconnects between innumerable devices. The IoT lets people living and working smarter by offering smart objects. Due to its importance, IoT is applied in many fields, as well as for water monitoring[1–5], healthcare[6–9], smart environment[10–13], smart home[14–19], and others. In fact, there is no standard architecture of IoT. However, according to Fig. 1, the architecture illustrated consists of three main layers, including perception layer, networking layer, and application layer. The first layer

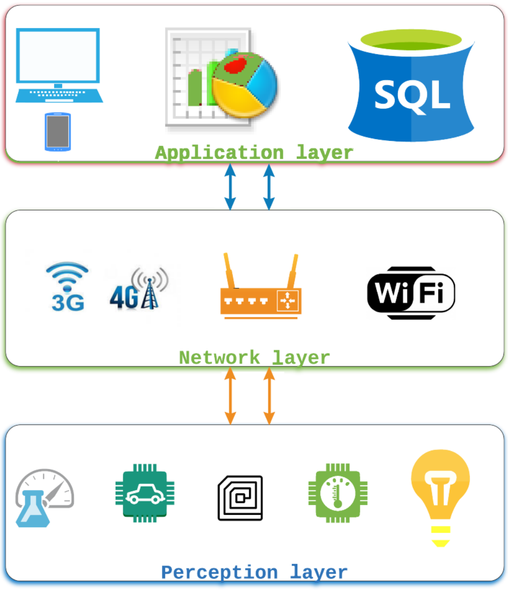


Fig. 1 Architecture of IoTs.

• Mourade Azrour and Yousef Farhaoui are with IDMS Team, Department of Computer Science, Faculty of Sciences and Techniques, Moulay Ismail University, Errachidia 52000, Morocco. E-mail: mo.azrour@umi.ac.ma; y.farhaoui@fste.umi.ac.ma.
• Jamal Mabrouki is with Laboratory of Spectroscopy, Molecular Modeling, Materials, Nanomaterial, Water and Environment, CERNE2D, Faculty of Science, Mohammed V University in Rabat, Rabat 10000, Morocco. E-mail: jamalmabrouki@gmail.com.
• Azedine Guezzaz is with Department of Computer Science and Mathematics, High School of Technology, Cadi Ayyad University, Marrakesh 40000, Morocco. E-mail: a.guzzaz@gmail.com.
∗ To whom correspondence should be addressed.
Manuscript received: 2020-06-08; accepted: 2020-07-01

is equipped with sensors and actuator for sensing and collecting data from their environment. The sensors can capture physical values, for example, vibration, motion, temperature, and humidity. The second layer has a role to transfer captured values and link between the various elements of the network. Many network solutions can be adopted in this layer, including Bluetooth, Wi-Fi, GSM, 4G/5G, Zigbee, Wimax, etc. For the application layer, it is responsible to process and store received data for the operators to develope the applications, for example, smart environment.

Currently, the number of linked things to the internet is growing very rapidly. According to the Gartner results, the total of linked objects by 2020 will be more than 20 billion[20]. As a result, our daily life is touched by IoT applications either in personal or in a full social order. So, IoT covers several fields, it makes our usual actions simple and alters the relationship between people and different objects[21].

Regardless of the great importance of IoT in our life, this technology has to resolve certain issues, for example, to link between hybrid resources and systems, the invention of new protocol is required. Furthermore, the security of private data must be satisfied and the security is considered as the most important issue, then it must receive great interest. The type of security that is required for IoT comprehends data integrity, the privacy protection, access control, service availability, and so on[22]. Therefore, it surpasses the standard security that enables to protect transferred data. Furthermore, the two mechanisms used in IoT for preventing unauthorized users and devices to access to the sensed and captured values are the authentication and access control.

For assuring this two security services, many researches have proposed various authentication protocols for IoT. Therefore, in recent years, Ye et al.[23] suggested a new authentication and key exchanging protocol for IoTs devices. So, they demonstrated that the protocol can resist against some attacks. However, Azrour et al.[24] demonstrated that the protocol in Ref. [23] is vulnerable to some attacks and it has many security problems. Accordingly, in this study, we propose an enhanced authentication protocol for IoT. Additionally, we expose the result of the comparative study between our proposed protocol and other correlated ones.

The rest of this paper is structured as follows. Section 2 is reserved for presenting the literature review. In Section 3, we detail our proposed IoT authentication protocol. The security analysis and performance comparison are given in Sections 4 and 5, respectively. Then the paper is concluded in Section 6.

2 Literature Review

Due to the importance of the security in IoT and the necessity of assuring the confidentiality of the user's data, the execution authentication protocol between connected devices is obligatory. Furthermore, in order to strengthen the authentication process, many specialists have presented different authentication protocol models based on various encryption techniques and algorithms.

In 2014, Jan et al.[25] presented an efficient authentication protocol that allows server and IoT objects to authenticate each other mutually. The protocol is based on shared key method to verify the identity of server and IoT devices, and also to share the secret key between two entities. In the later year, in order to secure the communication between IoT devices and cloud servers, Kalra and Sood[26] introduced a robust mutual authentication protocol that is founded on primitive of Elliptic Curve Cryptography (ECC)[27] and that uses HTTP cookies. After simulating their protocol under Automated Validation of Internet Security Protocols and Appplications (AVISPA) tools, they confirmed that their scheme can be used to provide the mutual authentication and it can resist against several attacks.

In 2017, Wu et al.[28] presented a new authentication protocol for IoT-based Wireless Sensor Networks (WSNs) which aims to resolve the recommended directives for IoT, that are introduced by Fantacci et al.[29] and Nguyen et al.[30]. For establishing the communication the user firstly sends a message to gateway, then the last one transfers it to the sensor. At the end, the user, gateway, and sensor authenticate each other mutually. Nevertheless, Bayat et al.[31] proved that the protocol in Ref. [28] is not very secured as it cannot deal with some security attacks. Consequently, for enhancing the protocol in Ref. [28], Bayat et al.[31] proposed a provable secure authentication protocol. They justified that the enhanced protocol is secured after the simulation under ProVerif analyzer.

In recent times, Li et al.[32] proposed a three-factor anonymous authentication protocol based on a fuzzy commitment protocol and error correction code to handle the user's biometric data. The protocol is applied for authenticate devices-based WSNs in IoT environments. They demonstrated that their scheme might guarantee computational efficiency and achieve more security and functional features. However, in 2019, Tai et al.[33] showed that the protocol in Ref. [32] is not secured against various attacks.

The quantum cryptography technic is also used by Sharma and Kalra[34] and Karla and Sood[26] for proposing two-factor authentication scheme to identify users and cloud servers. Hereafter, they demonstrated that their protocol is secured against possible attacks.

On the other hand, Dhillon and Kalra[35] suggested an authentication protocol for authenticating the identity both users and devices if they want have an authorized access to the patient information in healthcare application. Subsequently, they confirmed that their proposed protocol can resist against several attacks. Through using AVISPA tool, they determined that their scheme gets the wanted aims and it is protected against active and passive attacks.

3 Our Proposed Protocol

In this section, we detailed a new enhanced authentication protocol for IoTs. Our proposed protocol consists of four phases, which are new sensor adding phase, user registration phase, login and authentication phase, and password changing phase. The used notations are illustrated in Table 1.

3.1 New sensor addition phase

In order to add new sensor node Sn_i in an existing sensor network, the gateway generates random and particular $\mathrm{ID}_{\mathrm{Sn}}$ and K_{GSn_i} as identifier and key of the new sensor, respectively. Then, the gateway loads this information into the node memory before deployment. Hence, it stores $\mathrm{ID}_{\mathrm{Sn}}$, K_{GSn_i}, and its database for future usage.

Table 1 Symbolizations and their meanings.

Notation	Explanation
U	User
Sn_i	Sensor
GW	Gateway
$\mathrm{ID}_u/\mathrm{ID}_{\mathrm{Sn}}$	Identify of user/sensor
x_{Gw}	Gateway private key
PW_u	User's password
$E(a,b)$	Elliptic curve equation with order n
P	Point on $E(a,b)$
K_{GSn_i}	Secret key shared between GW and Sn_i
$h(\ )$	One way hash function
$\Vert$	String concatenation operator
$\oplus$	XOR operator
T_i	Timestamp ($i = 1, 2, \dots, 5$)

Note here that K_{GSn_i} is the secret key shared between the gateway and the sensor.

3.2 User registration phase

As depicted in Fig. 2, the user can register by performing registration phase through a secure channel as follows:

R1: The user U chooses his/her identity ID_u and the corresponding password PW_u. Then, he/she selects randomly two numbers r_1 and r_2. After that, it computes $\mathrm{HID} = h(\mathrm{ID}_u \Vert r_1)$ and $\mathrm{HPW} = h(\mathrm{ID}_u \Vert \mathrm{PW}_u \Vert r_2)$ that are sent to the gateway through a secure channel.

R2: The gateway GW selects a random number r_3 and computes $V = h(x_{\mathrm{Gw}} \Vert r_3)P \oplus \mathrm{HPW}$. Then, the gateway stores HID and r_3 in its database and sends V to user U.

R3: The user stores this information $\{V, r_1, r_2, \mathrm{HID}\}$ in the smartcard.

3.3 Login and authentication phase

In this phase, the communication is established among user, gateway, and sensor node through a public channel. The five steps of this phase are illustrated in Fig. 3 and are detailed as follows:

Auth1: $U \rightarrow \mathrm{GW}$: $\{\mathrm{HID}', V_{\mathrm{U1}}, T_1, a, \mathrm{ID}_{\mathrm{Sn}}\}$. After inputing the ID_u and PW_u, user U chooses a random integer a, computes $\mathrm{HID}' = h(\mathrm{ID}_u \Vert r_1)$, then checks if $\mathrm{HID}' \overset{?}{=} \mathrm{HID}$ or not. If it is ok, U computes $\mathrm{HPW}' = h(\mathrm{ID}_u \Vert \mathrm{PW}_u \Vert r_2)$ and $V_{\mathrm{U1}} = h(V \oplus \mathrm{HPW}' \Vert a)$. Finally, it sends this message $\{\mathrm{HID}', V_{\mathrm{U1}}, T_1, a, \mathrm{ID}_{\mathrm{Sn}}\}$ to the gateway.

Auth2: $\mathrm{GW} \rightarrow \mathrm{Sn}_i$: $\{V_{\mathrm{Sn1}}, \mathrm{HID}, T_2, b\}$. When user's message is received, the gateway verifies the timestamp $T_2 - T_1 \leqslant \Delta T$ and checks if $V_{\mathrm{U1}} \overset{?}{=} h(h(x_{\mathrm{Gw}} \Vert r_3)P \Vert a)$. If it is ok, the gateway chooses b as random integer and computes

$$V_{\mathrm{Sn1}} = h(\mathrm{HID} \Vert \mathrm{ID}_{\mathrm{Sn}} \Vert T_2 \Vert b \Vert K_{\mathrm{GSn}_i})P.$$

Lastly, the gateway send this information $\{V_{\mathrm{Sn1}}, \mathrm{HID}, T_2, b\}$ to the sensor node.

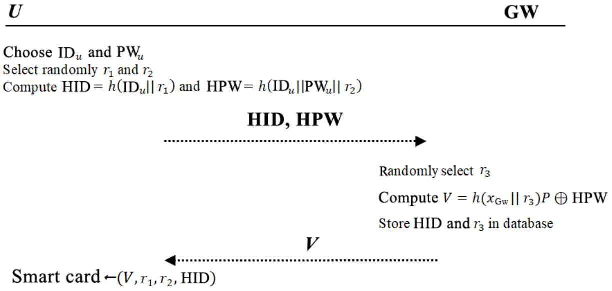

U
GW
Choose ID_u and PW_u
Select randomly r_1 and r_2
Compute $\mathrm{HID} = h(\mathrm{ID}_u \Vert r_1)$ and $\mathrm{HPW} = h(\mathrm{ID}_u \Vert \mathrm{PW}_u \Vert r_2)$
HID, HPW
Randomly select r_3
Compute $V = h(x_{\mathrm{Gw}} \Vert r_3)P \oplus \mathrm{HPW}$
Store HID and r_3 in database
V
Smart card ←$(V, r_1, r_2, \mathrm{HID})$

Fig. 2 Registration phase.

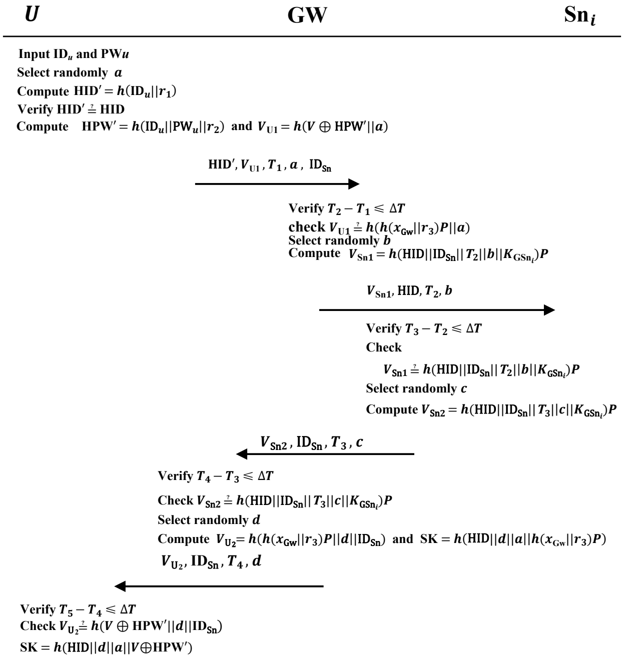

U
GW
Sn_i
Input ID_u and PWu
Select randomly a
Compute $\mathrm{HID}' = h(\mathrm{ID}_u||r_1)$
Verify $\mathrm{HID}' \overset{?}{=} \mathrm{HID}$
Compute $\mathrm{HPW}' = h(\mathrm{ID}_u||\mathrm{PW}_u||r_2)$ and $V_{\mathrm{U1}} = h(V \oplus \mathrm{HPW}'||a)$
$\mathrm{HID}', V_{\mathrm{U1}}, T_1, a, \mathrm{ID}_{\mathrm{Sn}}$
Verify $T_2 - T_1 \leqslant \Delta T$
check $V_{\mathrm{U1}} \overset{?}{=} h(h(x_{\mathrm{Gw}}||r_3)P||a)$
Select randomly b
Compute $V_{\mathrm{Sn1}} = h(\mathrm{HID}||\mathrm{ID}_{\mathrm{Sn}}||T_2||b||K_{\mathrm{GSn}_i})P$
$V_{\mathrm{Sn1}}, \mathrm{HID}, T_2, b$
Verify $T_3 - T_2 \leqslant \Delta T$
Check
$V_{\mathrm{Sn1}} \overset{?}{=} h(\mathrm{HID}||\mathrm{ID}_{\mathrm{Sn}}||T_2||b||K_{\mathrm{GSn}_i})P$
Select randomly c
Compute $V_{\mathrm{Sn2}} = h(\mathrm{HID}||\mathrm{ID}_{\mathrm{Sn}}||T_3||c||K_{\mathrm{GSn}_i})P$
$V_{\mathrm{Sn2}}, \mathrm{ID}_{\mathrm{Sn}}, T_3, c$
Verify $T_4 - T_3 \leqslant \Delta T$
Check $V_{\mathrm{Sn2}} \overset{?}{=} h(\mathrm{HID}||\mathrm{ID}_{\mathrm{Sn}}||T_3||c||K_{\mathrm{GSn}_i})P$
Select randomly d
Compute $V_{\mathrm{U_2}} = h(h(x_{\mathrm{Gw}}||r_3)P||d||\mathrm{ID}_{\mathrm{Sn}})$ and $\mathrm{SK} = h(\mathrm{HID}||d||a||h(x_{\mathrm{Gw}}||r_3)P)$
$V_{\mathrm{U_2}}, \mathrm{ID}_{\mathrm{Sn}}, T_4, d$
Verify $T_5 - T_4 \leqslant \Delta T$
Check $V_{\mathrm{U_2}} \overset{?}{=} h(V \oplus \mathrm{HPW}'||d||\mathrm{ID}_{\mathrm{Sn}})$
$\mathrm{SK} = h(\mathrm{HID}||d||a||V \oplus \mathrm{HPW}')$

Fig. 3 Login and authentication phase.

Auth3: $\mathrm{Sn}_i \rightarrow \mathrm{GW}$: $\{V_{\mathrm{Sn2}}, \mathrm{ID}_{\mathrm{Sn}}, T_3, c\}$. Upon receiving the message coming from the gateway, the sensor Sn_i verifies the timestamp $T_3 - T_2 \leqslant \Delta T$ and checks if $V_{\mathrm{Sn1}} \overset{?}{=} h(\mathrm{HID} \parallel \mathrm{ID}_{\mathrm{Sn}} \parallel T_2 \parallel b \parallel K_{\mathrm{GSn}_i})P$. If it is ok, the sensor randomly selects an integer c, and calculates the value of $V_{\mathrm{Sn2}} = h(\mathrm{HID} \| \mathrm{ID}_{\mathrm{Sn}} \| T_3 \| c \| K_{\mathrm{GSn}_i})P$. Then, the sensor replies back to the gateway by this message $\{V_{\mathrm{Sn2}}, \mathrm{ID}_{\mathrm{Sn}}, T_3, c\}$.

Auth4: $\mathrm{GW} \rightarrow U$: $\{V_{\mathrm{U2}}, \mathrm{ID}_{\mathrm{Sn}}, T_4, d\}$. Once the sensor's response is arrived, the gateway GW verifies the timestamp $T_4 - T_3 \leqslant \Delta T$ and checks if $V_{\mathrm{Sn2}} \overset{?}{=} h(\mathrm{HID} \| \mathrm{ID}_{\mathrm{Sn}} \| T_3 \| c \| K_{\mathrm{GSn}_i})P$. If it is valid, the gateway randomly picks an integer d, and calculates $V_{\mathrm{U2}} = h(h(x_{\mathrm{Gw}} \parallel r_3)P \parallel d \parallel \mathrm{ID}_{\mathrm{Sn}})$. Next, the gateway computes the session key, $\mathrm{SK} = h(\mathrm{HID} \parallel d \parallel a \parallel h(x_{\mathrm{Gw}} \parallel r_3)P)$. Then, the gateway responses back to the user by sending the following information $\{V_{\mathrm{U2}}, \mathrm{ID}_{\mathrm{Sn}}, T_4, d\}$.

Auth5: After receiving the gateway response, the user U validates the timestamp $T_5 - T_4 \leqslant \Delta T$ and tests if $V_{\mathrm{U2}} \overset{?}{=} h(V \oplus \mathrm{HPW}' \| d \| \mathrm{ID}_{\mathrm{Sn}})$. If it is valid, the user computes the session key, $\mathrm{SK} = h(\mathrm{HID} \| d \| a \| V \oplus \mathrm{HPW}')$.

3.4 Password changing phase

In order to change spontaneously his/her password through a public channel, the user has to execute the login and authentication phase with his/her ID_u and old password PW_u. Once getting the successful authentication and sharing the session key, the user chooses his new password PW_U^* as illustrated in Fig. 4, the details are as follows:

Change1: $U \rightarrow \mathrm{GW}$: $\{M_1\}$. The user inputs ID_u and PW_u, then checks $\mathrm{HID} \overset{?}{=} h(\mathrm{ID}_u \| r_1)$. In the case it is ok, it chooses freely his/her new PW_u^*, selects two random integers r_1^* and r_2^*, then calculates the values of $\mathrm{HID}^* = h(\mathrm{ID}_u \| r_1^*)$ and $\mathrm{HPW}^* = h(\mathrm{ID}_u \| \mathrm{PW}_u^* \| r_2^*)$. Next, it encrypts the message with the session key $M_1 = E_{\mathrm{SK}}(\mathrm{HPW} \| \mathrm{HPW}^* \| \mathrm{HID} \| \mathrm{HID}^* \| V)$. Finally, it sends message M_1 to the gateway.

Change2: $\mathrm{GW} \rightarrow U$: $\{M_2\}$. Upon receiving the user's message, the gateway decrypts it, $M_1' = D_{\mathrm{SK}}(\mathrm{HPW} \| \mathrm{HPW}^* \| \mathrm{HID} \| \mathrm{HID}^* \| V)$. Next, it checks if $V \overset{?}{=} h(x_{\mathrm{Gw}} \| r_3)P \oplus \mathrm{HPW}$. If it is ok, the gateway randomly selects an integer r_3^* and replaces HID and r_3 by HID^* and r_3^*. Afterward, it computes $V^* = h(x_{\mathrm{Gw}} \| r_3^*)P \oplus \mathrm{HPW}^*$ and encrypts V using the session key, $M_2 = E_{\mathrm{SK}}(V^*)$. This last one is sent back to user.

Change3: Once the gateway response is arrived, the user descripts $M_2' = D_{\mathrm{SK}}(V^*)$. Then, it replaces V, r_1, r_2, and HID with the new values V^*, r_1^*, r_2^*, and HID^*, respectively.

4 Security Analysis

4.1 Informal analysis

- **Mutual authentication**

  In the proposed scheme, the gateway authenticates the user and the sensor device. For the user, the gateway compares the value of V_{U1} received from the user with the computed $h(h(x_{\mathrm{Gw}} \| r_3)P \| a)$ in Auth2. For the sensor, in Auth4, the gateway checks the correctness

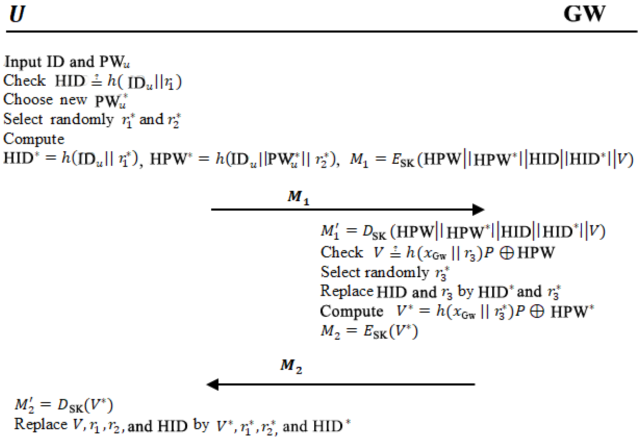

U
GW
Input ID and PW_u
Check $\mathrm{HID} \overset{?}{=} h(\mathrm{ID}_u||r_1)$
Choose new PW_u^*
Select randomly r_1^* and r_2^*
Compute
$\mathrm{HID}^* = h(\mathrm{ID}_u|| r_1^*)$, $\mathrm{HPW}^* = h(\mathrm{ID}_u||\mathrm{PW}_u^*|| r_2^*)$, $M_1 = E_{\mathrm{SK}}(\mathrm{HPW}||\mathrm{HPW}^*||\mathrm{HID}||\mathrm{HID}^*||V)$
M_1
$M_1' = D_{\mathrm{SK}}(\mathrm{HPW}||\mathrm{HPW}^*||\mathrm{HID}||\mathrm{HID}^*||V)$
Check $V \overset{?}{=} h(x_{\mathrm{Gw}}|| r_3)P \oplus \mathrm{HPW}$
Select randomly r_3^*
Replace HID and r_3 by HID^* and r_3^*
Compute $V^* = h(x_{\mathrm{Gw}}|| r_3^*)P \oplus \mathrm{HPW}^*$
$M_2 = E_{\mathrm{SK}}(V^*)$
M_2
$M_2' = D_{\mathrm{SK}}(V^*)$
Replace V, r_1, r_2, and HID by V^*, r_1^*, r_2^*, and HID^*

Fig. 4 Password changing phase.

of $V_{\mathrm{Sn2}} \overset{?}{=} h(\mathrm{HID} \parallel \mathrm{ID_{Sn}} \parallel T_3 \parallel c \parallel K_{\mathrm{GSn}_i})P$. On the other hand, the user can authenticate the server in Auth5, by checking the validity of $V_{\mathrm{U2}} \overset{?}{=} h(V \oplus \mathrm{HPW}' \| d \| \mathrm{ID_{Sn}})$. Finally, in Auth3, the sensor verifies the correctness of $V_{\mathrm{Sn1}} \overset{?}{=} h(\mathrm{HID} \| \mathrm{ID_{Sn}} \| T_2 \| b \| K_{\mathrm{GSn}_i})P$. If it is ok, the server is authenticated correctly. Accordingly, our proposed protocol offers mutual authentication.

- **Session key secrecy**

  Session key secrecy means that at the end of authentication phase and key exchange, anybody cannot know the session key excluding the user and gateway. In our proposed protocol, the session key is calculated in this way, $\mathrm{SK} = h(\mathrm{HID} \parallel d \parallel a \parallel h(x_{\mathrm{Gw}} \parallel r_3)P)$ or $\mathrm{SK} = h(\mathrm{HID} \parallel d \parallel a \parallel V \oplus \mathrm{HPW}')$, where $\mathrm{HPW}' = h(\mathrm{ID}_u \| \mathrm{PW}_u \| r_2)$. Since, PW_u, r_2, and ID_u are secret, the session key cannot be computed by anyone except the user and the gateway. For that reason, our proposed protocol provides session key secrecy.

- **Password guessing attack**

  Suppose that an attacker eavesdrops the communication between user U, gateway GW, and sensor Sn, then gets V_{U1}, where $V_{\mathrm{U1}} = h(V \oplus \mathrm{HPW}' \| a)$ and $\mathrm{HPW}' = h(\mathrm{ID}_u \| \mathrm{PW}_u \| r_2)$. For verifying the password, the attacker must know ID_u, r_2, and the value of V. Since, those values are not transmitted directly; the pirate cannot verify the correctness of guessed password. Therefore, our scheme can resist against password guessing attack.

- **Insider attack**

  Insider attack refers to a security risk in which a legitimate user or device executes a malicious code or tries to access to other account. In our proposed protocol, all session parameters are limited to a specific session. So, they are recomputed in every new session. Therefore, the insider (user or device) is not capable to execute the insider attack, due to it has no new parameters of other sessions. Therefore, our proposed protocol is secured against insider attack.

- **Replay attack**

  In our proposed scheme, in the case an adversary attempts to alter user's password, it needs to discover a session key and validate user ID. Even if the adversary has it or a valid user has not closed an old session, the adversary accesses to the user's application, it cannot modify the password without knowing the old one. For that reason, our proposed protocol is secured against replay attack.

- **Denning-sacco attack**

  Denning-sacco attack denotes the ability to have a long-term private key, like password, gateway private key, or the session key, through old session key. In our proposed scheme, the session key is calculated in this way,

  $$\mathrm{SK} = h(\mathrm{HID} \| d \| a \| h(x_{\mathrm{Gw}} \| r_3)P),$$

  where a and d are two random numbers generated for each session. Hence, it is impossible to get user password, because it is not used for generation session keys. Furthermore, it is hard to compute the private key of gateway from $h(x_{\mathrm{Gw}} \| r_3)P$, because the pirate has to face Elliptic Curve Cryptography Diffie-Hellman (ECCDH) and to get the secret random number r_3. Finally, we can say that the proposed scheme is resistant against denning-sacco attack.

- **Stolen verifier**

  In our proposed authentication protocol, any secret information, including user password or gateway secret key, is saved in the database. Therefore, the attacker is not capable to get correct user password, even if he gets an unauthorized access to the database. Besides, if he has accessed to the sensor, he cannot compute the session key K_{GSn_i}, as it depends on a random number. As a result, our proposed scheme is secure against stolen verifier attack.

- **Denial of Service (DoS) attack**

  For verifying the newly received message, we have used the time stamps. In addition, random values are generated in each step and in each session, and since the repetitive messages are not allowed, the pirate cannot execute the DoS attack messages. Consequently, our proposed protocol can deal with DoS attack.

4.2 Formal security analysis under scyther tool

In this section, we firstly explain the utility of scyther tool[36], which is used for formal security analysis of our protocol. Then, we present the obtained results under this tool. Scyther is a tool that is developed and designed for formal analysis security protocol under the perfect cryptography assumption. It can identify the security requirements and vulnerabilities of a given protocol. The algorithms developed in scyther tool can provide features, such as

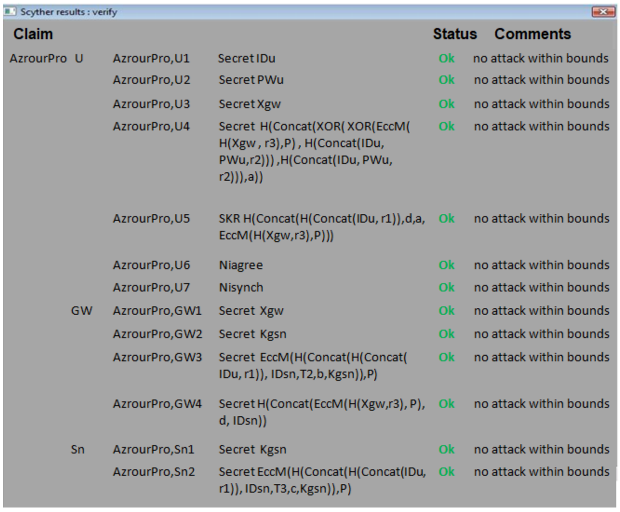
- Leading achievements, which have enabled new models for protocol analysis, including multi-protocol analysis.

- The powerful creation of a finite description of an unlimited number of model traces, also known as a full feature.

Our proposed scheme is then specified according to Security Protocol Description Language (SPDL). This specification describes the roles of user, gateway, and sensor. Each role includes sequences of events (send, receive, announcements, and claim events). Figure 5 illustrates the verification result obtained from our protocol under scyther tool. The result shows that our protocol satisfies all security requirements and no attack is found.

5 Performance Analysis

In this section, our proposed protocol is compared with other related ones. In this comparison, we have done our analysis according to the two points of views, the security and performance.



Claim				Status	Comments
AzrourPro	U	AzrourPro,U1	Secret IDu	Ok	no attack within bounds
		AzrourPro,U2	Secret PWu	Ok	no attack within bounds
		AzrourPro,U3	Secret Xgw	Ok	no attack within bounds
		AzrourPro,U4	Secret H(Concat(XOR(XOR(EccM(H(Xgw , r3),P) , H(Concat(IDu, PWu,r2))) ,H(Concat(IDu, PWu, r2))),a))	Ok	no attack within bounds
		AzrourPro,U5	SKR H(Concat(H(Concat(IDu, r1)),d,a, EccM(H(Xgw,r3),P)))	Ok	no attack within bounds
		AzrourPro,U6	Niagree	Ok	no attack within bounds
		AzrourPro,U7	Nisynch	Ok	no attack within bounds
	GW	AzrourPro,GW1	Secret Xgw	Ok	no attack within bounds
		AzrourPro,GW2	Secret Kgsn	Ok	no attack within bounds
		AzrourPro,GW3	Secret EccM(H(Concat(H(Concat(IDu, r1)), IDsn,T2,b,Kgsn)),P)	Ok	no attack within bounds
		AzrourPro,GW4	Secret H(Concat(EccM(H(Xgw,r3), P), d, IDsn))	Ok	no attack within bounds
	Sn	AzrourPro,Sn1	Secret Kgsn	Ok	no attack within bounds
		AzrourPro,Sn2	Secret EccM(H(Concat(H(Concat(IDu, r1)), IDsn,T3,c,Kgsn)),P)	Ok	no attack within bounds

Fig. 5 Scyther test results.

As illustrated in Table 2 and security analysis, our protocol is secured against stolen verifier attack, denning-sacco attack, password guessing attack, replay attack, DoS attack, and insider attack. Furthermore, it can provide mutual authentication and session key secrecy. On the other hand, Karla and Sood's[26] scheme is vulnerable to password guessing, DoS and insider attacks do not provide mutual authentication. The protocol in Ref. [37] cannot resist against replay and DoS attacks. The protocol in Ref. [38] is vulnerable against stolen verifier and insider attacks. Moreover, it is not able to provide session key secrecy. Finally, the scheme in Ref. [39] cannot resist against password guessing attack. The computation costs of our proposed protocol are compared with other related protocol. In this evaluation, very lightweight functions, such as string concatenation operation and XOR operation, are not neglected, because nearby calculation cost is slight. The symbolizations used are as follows:

- T_h: Computational charge of one-way hash operation;
- T_{pm}: Computational charge of elliptic curve point multiplication;
- T_{inv}: Computational charge of modular inversion;
- $T_{E/D}$: Computational charge of encryption and decryption algorithm.

In our protocol's authentication phase, the user computes $5T_h$, the gateway calculates $6T_h + 4T_{\text{pm}}$, and the sensor computes $2T_h + 2T_{\text{pm}}$. Therefore, the total computation cost of our protocol is $13T_h + 6T_{\text{pm}}$. According to Table 3, we can notice that modular inversion operation, symmetric encryption, and decryption algorithms are not used in our protocol, they

Table 2 Security performance.

Attack	Protocol in Ref. [26]	Protocol in Ref. [37]	Protocol in Ref. [38]	Protocol in Ref. [39]	Our protocol
Stolen verifier	√	×	×	√	√
Denning-sacco	√	√	–	√	√
Password guessing	×	√	–	×	√
Replay	√	×	√	√	√
DoS	√	×	–	√	√
Insider	×	√	×	√	√
Mutual authentication	×	√	–	√	√
Session key secrecy	√	√	×	√	√

Note: √: Yes ×: No

Table 3 Computational comparison.

Item	Computation cost in Ref. [40]	Computation cost in Ref. [41]	Computation cost in Ref. [42]	Computation cost in ours
User	$T_h + 2T_{\text{inv}}$	$11T_h$	$2T_h$	$5T_h$
Gateway	$4T_h + 4T_{\text{inv}}$	$11T_h$	$2T_h + T_E + T_D$	$6T_h + 4T_{\text{pm}}$
Sensor	$3T_h + 2T_{\text{inv}}$	$6T_h$	T_h	$2T_h + 2T_{\text{pm}}$
Total	$8T_h + 8T_{\text{inv}}$	$28T_h$	$5T_h + T_E + T_D$	$13T_h + 6T_{\text{pm}}$

are replaced by the ECC, which is very fast and offers same security. We can remark also that with our protocol, user computes only $5T_h$ and the sensor calculates just $2T_h + 2T_{\mathrm{pm}}$, consequently that is faster than the protocols in Refs. [40] and [42]. For that reason, we can say that our protocol is appropriate for IoTs applications.

6 Conclusion

In this paper, we recalled the vulnerabilities that we have discovered in protocol of Ref. [40]. Then, we proposed a new enhanced authentication protocol for IoTs applications. Afterwards, we analyzed our protocol informally and we justified that it can resist against various known attacks, including stolen verifier attack, denning-sacco attack, password guessing attack, replay attack, DoS attack, and insider attack. On the other hand, we have used scyther tool for analyzing the protocol formally, the obtained results confirm that our scheme can satisfy security requirements. Finally, we compared the performance and computation charges of the protocol with other related ones.

References

[1] J. Mabrouki, M. Azrour, Y. Farhaoui, and S. El Hajjaji, *Intelligent system for monitoring and detecting water quality*, in *Big Data and Networks Technologies*, Y. Farhaoui, ed. Springer International Publishing, 2020, pp.172–182.

[2] S. I. Samsudin, S. I. M. Salim, K. Osman, S. F. Sulaiman, and M. I. A. Sabri, A smart monitoring of a water quality detector system, *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 10, no. 3, pp. 951–958, 2018.

[3] N. Zidan, M. Maree, and S. Samhan, An IoT-based monitoring and controlling system for water chlorination treatment, in *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems–ICFNDS'18*, Amman, Jordan, 2018, pp. 1–6.

[4] B. Patil and D. J. Digge, Water quality monitoring in IoT environment, *International Organization of Scientific Research Journal of Engineering*, vol. 2, pp. 20–25, 2018.

[5] S. Pappu, P. Vudatha, A. V. Niharika, T. Karthick, and S. Sankaranarayanan, Intelligent IoT-based water quality monitoring system, *International Journal of Engineering Research and Applications*, vol. 12, no. 16, pp. 5447–5454, 2017.

[6] N. A. A. Bakar, W. M. W. Ramli, and N. H. Hassan, The Internet of Things in healthcare: An overview, challenges and model plan for security risks management process, *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 15, no. 1, pp. 414–420, 2019.

[7] N. Chawla, AI, IoT and wearable technology for smart healthcare – A review, *International Journal of Recent Research Aspects*, vol. 7, no. 1, pp. 9–13, 2020.

[8] M. S. Hossain, G. Muhammad, and A. Alamri, Smart healthcare monitoring: A voice pathology detection paradigm for smart cities, *Multimedia Systems*, vol. 25, no. 5, pp. 565–575, 2019.

[9] A. Kumar, G. Chattree, and S. Periyasamy, Smart healthcare monitoring system, *Wirel Pers Commun*, vol. 101, no. 1, pp. 453–463, 2018.

[10] D. W. Sukmaningsih, W. Suparta, A. Trisetyarso, B. S. Abbas, and C. H. Kang, Proposing smart disaster management in urban area, in *Intelligent Information and Database Systems*: *Recent Developments*, M. Huk, M. Maleszka, and E. Szczerbicki, eds. Springer International Publishing, 2020, pp. 3–16.

[11] X. Wei, N.-B. Chang, K. Bai, and W. Gao, Satellite remote sensing of aerosol optical depth: Advances, challenges, and perspectives, *Critical Reviews in Environmental Science and Technology*, vol. 50, no. 16, pp. 1640–1725, 2020.

[12] B. Bayat, N. Crasta, A. Crespi, A. M. Pascoal, and A. Ijspeert, Environmental monitoring using autonomous vehicles: A survey of recent searching techniques, *Current Opinion in Biotechnology*, doi: 10.1016/j.copbio.2017.01.009.

[13] A. Kulkarni and D. Mukhopadhyay, Internet of Things-based weather forecast monitoring system, *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 9, no. 3, pp. 555–557, 2018.

[14] H. Sayuti, R. A. Rashid, N. M. A. Latiff, M. R. A. Rahim, and N. E. Ghazali, Smart home and ambient assisted living based on the Internet of Things, *International Journal of Electrical & Computer Engineering*, vol. 7, no. 3, pp. 1480–1488, 2017.

[15] W. M. Kang, S. Y. Moon, and J. H. Park, An enhanced security framework for home appliances in smart home, *Human-centric Computing and Information Sciences*, vol. 7, no. 1, pp. 1–12, 2017.

[16] B. L. R. Stojkoska and K. V. Trivodaliev, A review of Internet of Things for smart home: Challenges and solutions, *Journal of Cleaner Production*, vol. 140, no. 3, pp. 1454–1464, 2017.

[17] X. Hong, C. Yang, and C. Rong, Smart home security monitor system, *International Symposium on Parallel & Distributed Computing*, doi: 10.1109/ISPDC.2016.42.

[18] M. A. E.-L. Mowad, A. Fathy, and A. Hafez, Smart home automated control system using android application and microcontroller, *International Journal of Scientific & Engineering Research*, vol. 5, no. 5, pp. 935–939, 2014.

[19] M. Soliman, T. Abiodun, T. Hamouda, J. Zhou, and C.-H. Lung, Smart home: Integrating Internet of Things with web services and cloud computing, doi: 10.1109/CloudCom.2013.155.

[20] Smarter with Gartner, The IoT effect: Opportunities and challenges, https://www.gartner.com/smarterwithgartner/the-iot-effect-opportunities-and-challenges-2/, 2018.

[21] A. Osseiran, O. Elloumi, J. Song, and J. F. Monserrat, Internet of Things, *IEEE Communications Magazine*, vol. 1, no. 2, p. 84, 2017.

[22] A. Sedrati and A. Mezrioui, A survey of security challenges in Internet of Things, *Advances in Science Technology and Engineering Systems Journal*, vol. 3, no. 1, pp. 274–280,

2018.

[23] N. Ye, Y. Zhu, R. Wang, R. Malekian, and L. Qiao-min, An efficient authentication and access control scheme for perception layer of Internet of Things, *Applied Mathematics & Information Sciences*, vol. 8, no. 4, pp. 1617–1624, 2014.

[24] M. Azrour, M. Ouanan, Y. Farhaoui, and A. Guezzaz, Security analysis of Ye et al. authentication protocol for Internet of Things, in *Big Data and Smart Digital Environment*, Y. Farhaoui and L. Moussaid, eds. Springer International Publishing, 2019, pp. 67–74.

[25] M. A. Jan, P. Nanda, X. He, Z. Tan, and R. P. Liu, A robust authentication scheme for observing resources in the Internet of Things environment, doi: 10.1109/TrustCom.2014.31.

[26] S. Kalra and S. K. Sood, Secure authentication scheme for IoT and cloud servers, *Pervasive & Mobile Computing*, vol. 24, pp. 210–223, 2015.

[27] V. S. Miller, Use of elliptic curves in cryptography, doi:10.1007/978-1-4939-1711-2_6.

[28] M. Wu, J. Chen, and R. Wang, An enhanced anonymous password-based authenticated key agreement scheme with formal proof, *International Journal of Network Security*, vol. 19, no. 5, pp. 785–793, 2017.

[29] R. Fantacci, T. Pecorella, R. Viti, and C. Carlini, A network architecture solution for efficient IOT WSN backhauling: Challenges and opportunities, *IEEE Wireless Communications*, vol. 21, no. 4, pp. 113–119, 2014.

[30] K. T. Nguyen, M. Laurent, and N. Oualha, Survey on secure communication protocols for the Internet of Things, *Ad Hoc Networks*, vol. 32, pp. 17–31, 2015.

[31] M. Bayat, M. Beheshti-Atashgah, M. Barari, and M. R. Aref, Cryptanalysis and improvement of a user authentication scheme for Internet of Things using elliptic curve cryptography, *IJ Network Security*, vol. 21, no. 6, pp. 897–911, 2019.

[32] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments, *Journal of Network and Computer Applications*, vol. 103, pp. 194–204, 2018.

[33] W.-L. Tai, Y.-F. Chang, and P.-L. Hou, Security analysis of a three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments, *IJ Network Security*, vol. 21, no. 6, pp. 1014–1020, 2019.

[34] G. Sharma and S. Kalra, A secure remote user authentication scheme for smart cities e-governance applications, *Journal of Reliable Intelligent Environments*, vol. 3, no. 3, pp. 177–188, 2017.

[35] P. K. Dhillon and S. Kalra, Multi-factor user authentication scheme for IoT-based healthcare services, *Journal of Reliable Intelligent Environments*, vol. 4, no. 3, pp. 141–160, 2018.

[36] C. J. F. Cremers, The scyther tool: Verification, falsification, and analysis of security protocols, doi: 10.1007/978-3-540-70545-1_38.

[37] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers, *The Journal of Supercomputing*, vol. 74, no. 12, pp. 6428–6453, 2018.

[38] W.-B. Hsieh and J.-S. Leu, A robust user authentication scheme using dynamic identity in wireless sensor networks, *Wireless Personal Communications*, vol. 77, no. 2, pp. 979–989, 2014.

[39] C.-C. Chang and H.-D. Le, A provably secure, efficient, and flexible authentication scheme for Ad Hoc wireless sensor networks, *IEEE Wireless Communications*, vol. 15, no. 1, pp. 357–366, 2016.

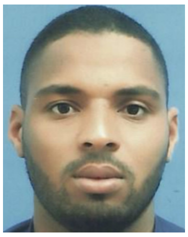
[40] H. L. Yeh, T. H. Chen, P. C. Liu, T. H. Kim, and H. W. Wei, A secured authentication protocol for wireless sensor networks using elliptic curves cryptography, *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011.

[41] A. K. Das, A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks, *Peer-to-Peer Networking and Applications*, vol. 9, no. 1, pp. 223–244, 2016.

[42] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. Najmus Saqib, Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key, *International Journal of Communication Systems*, vol. 32, no. 16, pp. 1–18, 2019.

Mourade Azrour received the PhD degree from Faculty of Sciences and Technologies, Moulay Ismail University, Errachidia, Morocco in 2019, and the MS degree in computer and distributed systems from Faculty of Sciences, Ibn Zouhr University, Agadir, Morocco in 2014. He currently works as a computer science professor at the Department of Computer Science, Faculty of Sciences and Technologies, Moulay Ismail University. His research interests include authentication protocol, computer security, Internet of Things, and smart systems. He is a scientific committee member of numerous international conferences. He is also a reviewer of various scientific journals, such as *International Journal of Cloud Computing* and *International Journal of Cyber-Security and Digital Forensics* (*IJCSDF*).

Yousef Farhaoui received the PhD degree in computer security from Ibn Zohr University of Science, Morocco in 2012. He is now a professor at Faculty of Sciences and Techniques, Moulay Ismail University. His research interests include e-learning, computer security, big data analytics, and business intelligence. He is a member of various international associations. He has authored 4 books and many book chapters with reputed publishers, such as Springer and IGI. He is served as a reviewer for IEEE, IET, Springer, Inderscience, and Elsevier journals. He is also the guest editor of many journals with Wiley, Springer, Inderscience, etc. He has been the general chair, session chair, and panelist in several conferences.



Azidine Guezzaz received the MS degree in the field of computer science and distributed systems from Department of Mathematics and Computer Science, Faculty of Science, University Ibn Zohr, Agadir, Morocco in 2013. He received the PhD degree from Faculty of Science, University Ibn Zohr, Agadir, Morocco in 2018. He was a professor at the Technology High School and BTS in the period 2014–2018. He then joined Cadi Ayyad University in 2018 as an assistant professor. His main field of research interests are intrusion detection and prevention, computer and network security, and cryptography.

Jamal Mabrouki received the PhD degree in water science and technology from Faculty of Sciences, Mohamed V University in Rabat, Morocco in 2020. He is an engineer in environment and climate. He is working on the project of migration and water and has the role of water governance in migration policy in Africa with the cooperation between MedYWat and World Bank. He is currently a researcher for the environment and climate program at ECOMED in Morocco, where he started the coordinator of the project "Adaptation of Citizens to Climate Change".