EAI Endorsed Transactions
on Cloud Systems
Research Article EAI.EU

AuthenIoT: A Lightweight Authentication Protocol for the Internet of Things Based Wireless Sensor Networks

Haythem Hayouni*

SupCom, University of Carthage, Tunisia

Abstract

The Internet of Things is a major development in information technology that increasingly dominates and reigns in the computer systems market. However, due to the threat of cyber attacks, the security of IoT is still one of the major issues holding back the evolution of this technology. For this, the authentication of objects is very important in IoT. In this paper, we propose a lightweight authentication protocol for the IoT Based Wireless Sensor Networks, called AuthenIoT. The objective is to provide mutual authentication services for connected objects. This protocol must take into account the constraints of the objects and the used communication technologies. To achieve such protocol, we opted for WSNs as an IoT use case. Furthermore, we demonstrate that the proposed scheme provides an efficient security for connected devices and that its computation and communication costs are suitable for extremely low-cost IoT devices.

Keywords: IoT, Security, WSNs, Authentication, Access control

Received on 12 September 2021, accepted on 01 October 2021, published on 14 October 2021

doi: 10.4108/eai.14-10-2021.171321

1. Introduction

The Internet of Things (IoT) [1] represents a major part of our daily life. Billions of intelligent and autonomous objects around the world are connected and communicate with each other. Its success is due to the evolution of hardware equipment and communication technologies including wireless. IoT is the result of the development and combination of different technologies. It encompasses almost all areas [2] of current Information Technology such as smart cities, computer systems, connected vehicles, etc. And exploits other advanced technologies [3,4] such as Cloud Computing, Big Data, or even the blockchains. By definition, an object (Device) is a physical or virtual machine, which must be: (1) intelligent, therefore she must have a certain capacity for calculation and memorization. (2) autonomous, that is say that she can do treatments and sometimes even make decisions without a human intervention. (3) which can be connected with any other object of a flexible and transparent way. Wireless sensor networks (WSNs) are a cornerstone of the success of the IoT. Because by using small objects which are generally limited in terms of calculation capacity, memorization and energy, industrial, medical, agricultural, and other environments can be covered and managed automatically.

The Prosperity of IoT can only be achieved when we ensure good security for devices [5] and communication networks used which managed by an entity with no limited resources whose main role is the management of a network called CPAN. It is essential to put in place a policy of security that prevents any malicious or unauthorized object [6,7,8] from giving access to IoT systems, to read or modify their data. For an object to have the possibility of exploiting a service or to join a network, he must first prove his identity and have the rights necessary access. Connected objects are generally very limited in their capacity to calculation and storage. They are also constrained by energy consumption. Therefore, conventional security mechanisms [9] such as

* Email: haythem.hayouni@supcom.tn

authentication with digital certificates or the use of asymmetric cryptographic algorithms like RSA or Diffie-Hellman, cannot be used because they are very expensive, even not supported by the objects. Therefore, a new lightweight and robust mechanism must be created, which provides object authentication and data protection services, while being adapted to the capabilities of objects and communication technologies.

For these reasons, we propose in this paper a lightweight authentication protocol for the IoT Based Wireless Sensor Networks, called AuthenIoT. The objective is to provide authentication services for connected objects. This protocol must take into account the constraints of the objects and the used communication technologies. To achieve such protocol, we opted for WSNs [10] as an IoT use case. This choice is motivated by (1) the great success and the strong deployment of WSNs in various sectors. And also (2) by their evolutions and their continuous developments. We used a technology called OCARI. As is the case with several IoT and WSN systems, an OCARI network is made up of a set of subnets, where each is managed by a main entity (CPAN). So that a device can be joined to a network and exchange data, it must establish an association phase with the network's CPAN. Our protocol provides a mutual authentication between the device and the CPAN followed by an association phase, to protects the integrity of exchanged data.

The main contributions of this paper are as follows:

- We present a survey of authentication protocols published in recent years that deal with the IoT based WSNs are briefly presented and discussed.
- We propose a lightweight authentication protocol for the IoT Based Wireless Sensor Networks, called AuthenIoT, to provide authentication services for connected objects. AuthenIoT provides a mutual authentication between the device and the CPAN followed by an association phase, to protects the integrity of exchanged data
- We demonstrate that our protocol is secure against various kinds of known attacks by reporting on an informal security analysis
- We provide a comparison of performance between our protocol and related protocols. Several simulation tests have been performed to prove that our proposed protocol AuthenIoT achieves the desired security and efficiency requirements.

The remainder of this paper is organized as follows. An overview of the related work is presented in Section 2. The system model such as network and attack models are discussed in Section 3. In Section 4, we present our proposal protocol. A security analysis is performed and presented in Section 5. In Section 6, we evaluate the performance of our protocol. Finally, we draw our conclusions, and propose future enhancements in Section 7.

2. Related works

Compared to objects used in the classic Internet - which mainly represent computers - objects in the IoT represent all electronic equipment having a calculation and storage capacity, whether it is a very limited sensor in terms of performance and power consumption, or a large powered data center, with ultra-powerful capabilities. Because of this diversity of objects, it is difficult to design a robust security protocol that is at the same time suitable for these varied objects. In more, the fact that the trend in the IoT is to use wireless communication technologies makes the IoT system even more vulnerable and more exposed to all kinds of cyberattacks. In order to secure IoT systems, and ensure the properties seen above, it is necessary to design a protocol based on robust algorithms, but at the same time lightweight and flexible [22] [24]. This protocol must be adapted to different types of object, from the most powerful to lower, without there being a degradation in terms of security performance. In this section, we present and discusses some proposed authentication protocols for IoT based WSNs.

In [11], authors propose an authentication mechanism to secure communication in WSNs for IoT systems. This mechanism allows a sensor node in an identity-based cryptography to send a message to an Internet host in a public key infrastructure. However, the use of random nonce generated by the authentication initiator instead of the authenticator responder can create a security breach. Indeed, this flaw can be exploited to generate a replay attack which generates a denial of service.

A novel authentication scheme for multi-gateway based WSNs for IoT systems is proposed in [12]. Indeed, for the authentication a device must take a random number generated by the CPAN. As for the authentication of the device, it is based on an authentication token. This token is based on a sequence number that protects it against replay attacks. However, the generation of a large number of keys require a significant amount of storage, and consumes energy.

In [13], the authors propose an authentication protocol to provide an efficient association between a device and the CPAN. The authors provide two models to ensure the association in the IoT system. An entity wishing to communicate must first negotiate the security policy with the access point. Second, once they agree on the parameters supported by both parties, they must authenticate each other and generate session keys using two types of negotiations. However, this protocol is lightweight and does not use complicated algorithms, so it is possible to perform a Dos attack on users wanting to associate with the network.

In [14], an authentication mechanism, called WSN-SLAP, is proposed which based on the creation of secure channel between a user and the sensor node via a gateway

(e.g. CPAN). The authors develop this protocol based on the idea of the association of Home GWN and local sensor nodes. HGWN should contact all local sensor nodes. Its operating principle is summed up by the made that one party presents a challenge and another party must provide a valid response (calculated from a shared secret and a hash function) to be authenticated. Thanks to its performance, this method is very suitable for the IoT system, however the key management mechanism deployed in this protocol limits its flexibility and performance, and generates security vulnerabilities.

3. System model

In this section, we present the network and attack model for our proposed protocol.

3.1. Network model

To achieve such an approach, we opted for WSNs as the IoT use case. This choice is motivated by (1) the great success and the strong deployment of wireless sensor networks in different sectors (e.g. industrial, environmental, medical, military). And also (2) by their evolutions and their continuous developments. We used a technology called OCARI [15]. As is the case with several IoT and WSN systems [23][25], an OCARI network is made up of a set of subnets, where each is managed by a main entity (CPAN), which presented in Figure 1. In order for a device to join a network and exchange data, it must establish an association phase with the network's CPAN.

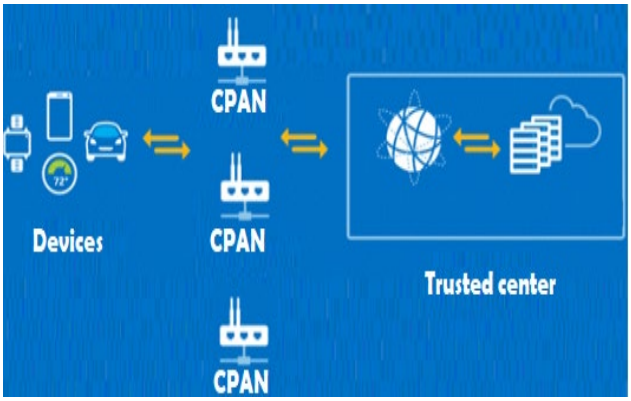

Figure 1. Network model of proposed protocol

3.2. Attacks model

In order to properly analyse our protocol against attacks, we have created an attack model, which represents a security protocol analysis procedure in order to identify its objectives and vulnerabilities. To do this, we have opted for the model of DolevYao [16] which represents the most used model. This model assumes that the network is formed by a set of entities that exchange data with each other (communication between a device and a CPAN) using wireless communication technology which may packets losses. It is also assumed that entities communicate in an unsecured environment. This environment contains attackers which capture, modify, interrupt, replay, forge, and reorder messages. These attacks are explained as follows:

- *Replay attack*: this is when a malicious user copies and sends back one or more messages already transmitted in order to exploit the system security;
- *Spoofing attack*: this is when a malicious entity succeeds in impersonating another, thereby giving access rights and benefits from the victim;
- *Brute force attack*: the principle of these attacks consists in testing a large number of passwords in the hope of detect the correct one. It can also be a data decryption operation where the attacker tries all possible keys until the correct key is found;
- *DoS*: this attack aims to make an unavailable resource or information. It can be achieved (1) by flooding the source or the network by a large number of messages, or (2) by exploiting a vulnerability in the protocol.

In our attack model, we assume that the stored secret information is protected and is cannot be physically stolen.

4. Proposed algorithm

In this section, we propose a protocol that contains a device authentication and association mechanisms and a data integrity protection service. The authentication mechanism is fast and robust. It helps protect systems against replay and cryptanalysis attacks. The principle of key generation of shared key ensures an optimal key management, protects the network against internal attacks, and provides flexibility and transparency with respect to adding new objects. In this section, we propose a novel protocol of authentication and association of devices in IoT environment. Each communication between two objects requires an association phase. Usually in WSNs, so that an object A can be associated with a managed network by an object B, A must send an association request to B, and the latter sends back an association response. However, any malicious object C can pretend to be A and impersonate it. To overcome this problem, it is essential to implement an authentication mechanism. We opted for an approach based on the One Time Password (OTP) mechanism which is defined in RFC 2289 [17] and RFC 4226 [18]. Through definition, an OTP is a password that is valid only once. Therefore, it is very robust against replay and cryptanalysis attacks. It can be used in synchronous or asynchronous mode. Our approach uses the asynchronous mode which is based on the challenge/response. We chose this mode because it does not require any prior approval between

communicating objects. Unlike synchronous mode requires agreement between objects on certain parameters such as the One-Time Password algorithm (TOTP) or the HMAC-based One-time Password (HOTP). Therefore, we calculate our OTP by combining the challenge/response method with HOTP [18] as described in Algorithm 1. We call the function that generates the OTP: FN_{OTP}

Algorithm 1 Calcul of OTP (FN_{OTP})

1: H=HMAC-SHA256(K, C);
2: I=F(H);
3: $E_1 = 4_{bytes}$ (I,H);
4: $E_2 = E_1 \wedge 0 \times 7F$
5: OTP= E_2 mod 8

First we calculate a hash function H which is a sequence of 32 bytes using the HMAC SHA-256 algorithm. H contains as input data a 32-byte secret key K and a 32-byte challenge C which represents a random number received from the authenticator. Then, via a function F we can have an index called I. Indeed, F takes the 4 low-order bits of the last byte of the obtained hash H. For example, if the value of H is:
D7|F6|09|E3|51|3F|AA|5C|19|4D|98|2B|A2|EB|C3|C6|84|70|A4|E8|EB|58|B7|DD|56|3A|7E|53|83|AF|69|BC, the last byte of H is equal to 0×BC then the 4 low-order bits represent 0×0C (12 based 10) and therefore I= 12. Then, by taking 4 bytes of the H from I which gives an unsigned integer E_1 = 0×22EBC3C6. Finally, to make sure that the size of the OTP is equal to 4 bytes, we do:

$$OTP = E_2 \ mod \ 8 \quad (1)$$

For our example, the OTP is 0×22EBC3C6.
Our proposed authentication and association in presented in Figure 2.

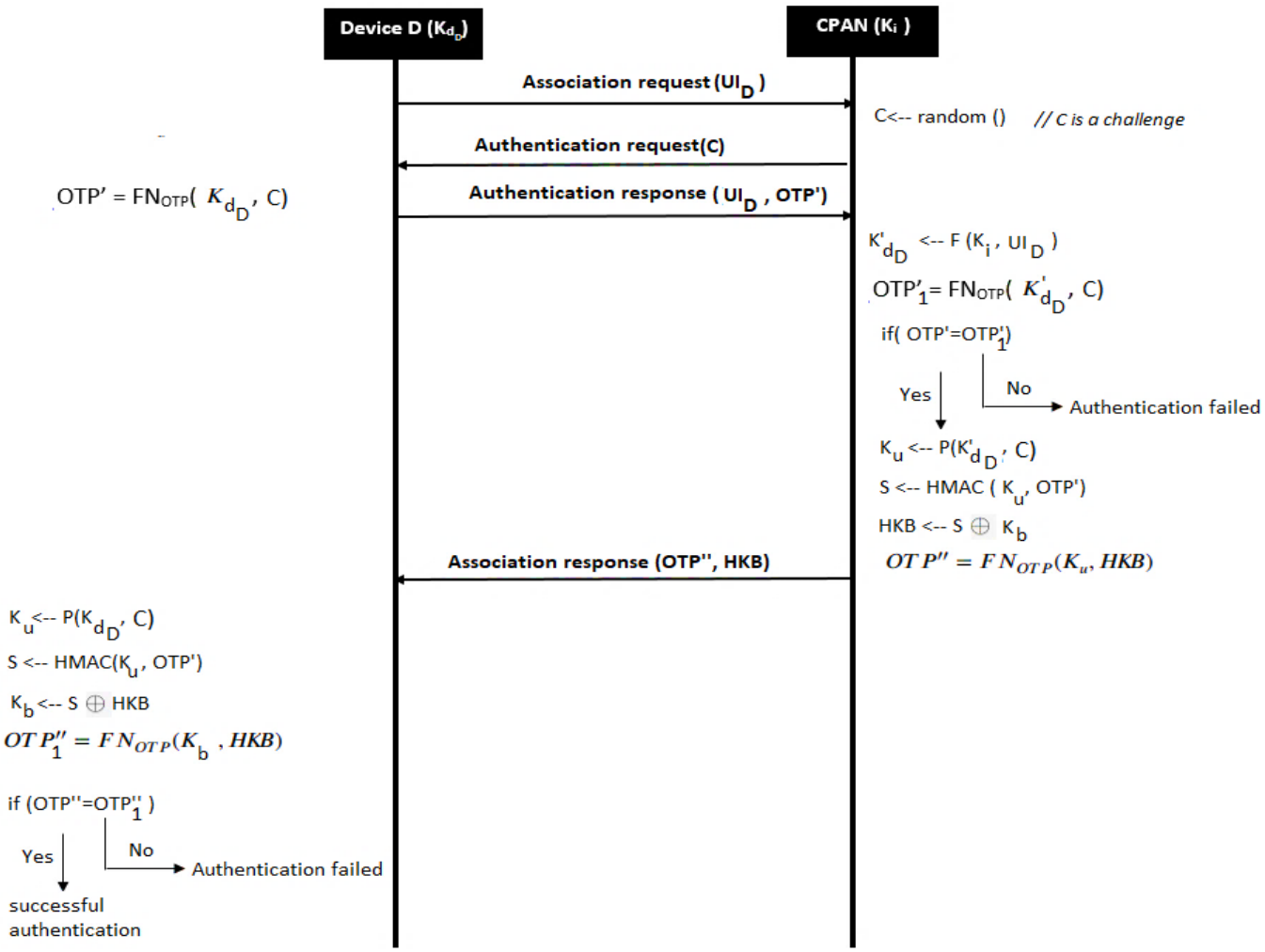

Figure 2. Our proposed protocol AuthenIoT

First, the device D makes an association request to CPAN containing its UI_D identifier. The CPAN generates it a challenge C, using a random function, and sends it with a message via an authentication request. Upon receipt of the

request, the device D calculates the OTP using the received challenge and K_{dD} as input data, then sends the result, associated with UI_D, to the CPAN via an authentication response. Second, the CPAN generates a derived key K'_{dD} corresponding to the device D, and calculates the OTP' based on K'_{dD} and the challenge C. After, the CPAN compares OTP' to the OTP generated by the device D, if the verification failed it will be rejected, otherwise the CPAN generates a key K_u which will be used to ensure the integrity of the data exchanged over a communication channel (session). K_u is only valid during a single session; this protects our protocol against cryptanalysis attacks. K_u is generated as follows, by using Pseudo Random Function P defined in RFC 5246 [19] which allows to have very robust keys:

$$K_u = P(K'_{d_D}, C) \quad (2)$$

The generation of keys is only established after successfully completing the authentication phase to avoid unnecessary calculations.

In our proposal, we also added a secure exchange mechanism of the broadcast key K_b, called HKB, and a computation of a second OTP (OTP") for CPAN authentication. The hidden key broadcast mechanism is carried out in 2 phases. (1) We generate a signature S by calculating a HMAC between the key K'_{dD} and the generated OTP', then, (2) we applies a XOR between the result and K_b:

$$S = HMAC\ (K'_{d_D}, OTP') \quad (3)$$

$$HKB = S \oplus K_b \quad (4)$$

$$OTP'' = FN_{OTP}(K_u, HKB) \quad (5)$$

OTP" is calculated by CPAN to make to objectives. First, to protect the integrity of HKB. Second, to ensure the authentication of CPAN. The generation of OTP" requires a secret and a unique challenge. Finally, the CPAN sends the couple (OTP", HKB) to device D as association response. When D receives this association response, it calculates K_u and the signature, and applicate the XOR between the signature and HKB in order to retrieve K_b which needs to be examined by checking its integrity. After, D calculate an OTP and compare it to the OTP" received from the CPAN. If the two OTPs match, so (1) it proves that HKB is not tampered with, and therefore the K_b is correct, and (2) the CPAN is authenticated. Otherwise, if OTP" or HKB or both are not correct or changed during their transmission, then the two OTPs do not match, therefore K_b is not accepted, the CPAN is rejected, and the bind operation fails. Having a correct OTP" proves the validity of the identity of CPAN.

5. Security analysis

In this section, we perform a security analysis of the proposed scheme under the introduced attacker model to prove that it is secure against the various attacks, and we verify the robustness and security of our protocol through formal validation using a tool of the automatic verification of security protocols.

5.1. Informal security analysis

5.1.1. Replay attack

During the association phase, the fact that the OTP is only valid for one use, protects the system from malicious users who try to resend replay the same messages in order to have unauthorized use of the system. In the data exchange phase via the secure channel, the data packets use sequence numbers, and since two packets cannot have the same number, no replay attack may be possible.

5.1.2. Spoofing attack

The two communicating entities authenticate each other using OTPs. These OTPs are based on pairs of secret information (not known to the attacker) and by a unique pseudo-random number valid only for a single use ((K_d , Challenge) for OTP' , and (K_u , HKB) for OTP"). Beside, K_d and K_u (derived from K_d) are linked to the object identifier. Therefore, a node without a custom key cannot be authenticated or impersonate a legitimate user

5.1.3. Brute force attack

Recovering keys by a brute force attack is almost impossible. According to [20], finding a 96 bits' password using hardware with good performance can take 2 centuries. The probability Pr of finding the right key K_d of 256 bits on the first move is $\Pr = \frac{1}{2^{256}}$, and for K_b and K_u of 128 bits is $\Pr = \frac{1}{2^{128}}$.

5.1.4 DoS

During the association phase, K_i is only used for internal operations of CPAN for the generation of K_d, and K_d is never used without a random or pseudorandom number and a hash function. In addition, the communication channel is based on a very robust ephemeral session keys and counters. Therefore, it protects the system against any cryptanalysis attack which can be deployed to recover keys or exchanged data.

5.2. Formal validation

In order to verify the robustness and security of our proposed protocol, we performed a formal validation using an automatic security protocol verification tool called Scyther [21]. In the formal language of Scyther, each protocol is defined by roles. Each role must be played by an agent and described by a sequence of events (send, receive, etc.). In the following, we present the structure of our source code (Figure 3).

```
protocol AuthenIoT (D,CPAN)
{
...
function FN_OTP ;
macro OTP' = FN_OTP(K (D, CPAN), challenge) ;  // K is the Key generated between D and CPAN
macro K_u= P(k(D,CPAN), challenge) ;
macro otp''= FN_OTP(K_u, HKB);
hashfunction HAMC ;
 macro S = HMAC(K_u,otp') ;
function HiddeBroadCastKey ;
function RevealBroadCastKey ;
const deviceAuthenticationError : String ;
const cpanAuthenticationError : String ;
```

AuthenIoT represents the name of the protocol, function and macro are used, respectively, for the definition of functions and the abbreviation of formulas. We have two roles played by the device D and the CPAN (Figure 4 and Figure 5). The different operations data transmission times are defined by the two events send and receive. The match event is used for model equality tests. The types of the claim event represent the purposes of formal validation. To validate the confidentiality of data transmissions, the secret "claim" is used. We also used 3 "claim" for validate authentication, which are Alive (for existence), Weakagree (for an agreement weak) and Niagree (for a non-injective agreement).

```
role D {
recv_1(CPAN,D,challenge) ;
send_2(D,CPAN,OTP') ;
 recv_3(CPAN,D,(receivedOtp'' ,HKB));
match(receivedOtp'',OTP'') ; // Successful authentication
macro KEY = RevealBroadCastKey(S ,HKB); // KEY is a broadcast key
claim (D, K_u) ;
claim (D, KEY) ;
claim (D, Alive) ;
 claim (D, Weakagree) ;
claim (D, Niagree) ;
}
```

Figure 4. Role of device D

```
role CPAN {
send_1(CPAN,D,challenge) ;
recv_2(D,CPAN,receivedOtp') ;
match (receivedOtp',OTP') ; // Successful authentication
macro HKB = HiddeBroadCastKey(S, KEY);
send_3(CPAN,D,(OTP'' ,HKB));
claim (CPAN, K_u) ;
claim (CPAN, KEY) ;
claim (C, Alive) ;
claim (C, Weakagree) ;
claim (C, Niagree) ;
};
```

Figure 5. Role of CPAN

columns ("Status" and "Comments") show the result of the verification process ("Fail" or "Ok") along with a short description. The result "No attack within bounds" should be interpreted as "Scyther found no attack when reaching the limit on the number of executions". As we can see, validation proves the security of our protocol.

Claim				Status	Comments
AuthenIoT	D	AuthenIoT, D1	P(k(D,CPAN), challenge)	Ok	No attacks within bounds.
		AuthenIoT, D2	RevealBroadCastKey(S ,HKB)	Ok	No attacks within bounds.
		AuthenIoT, D3	Alive	Ok	No attacks within bounds.
		AuthenIoT, D4	Weakagree	Ok	No attacks within bounds.
		AuthenIoT, D5	Niagree	Ok	No attacks within bounds.
	CPAN	AuthenIoT, CPAN1	P(k(D,CPAN), challenge)	Ok	No attacks within bounds.
		AuthenIoT, CPAN2	RevealBroadCastKey(S ,HKB)	Ok	No attacks within bounds.
		AuthenIoT, CPAN3	Alive	Ok	No attacks within bounds.
		AuthenIoT, CPAN4	Weakagree	Ok	No attacks within bounds.
		AuthenIoT, CPAN5	Niagree	Ok	No attacks within bounds.

Figure 6. Formal validation results of our protocol

6. Performance evaluation

In this section, we evaluate the performance of our protocol in terms of association delay and energy consumed during association phase. We compare our protocol to approach WSN-SLAP [14]. The simulation is made by the Network Simulator 3 (NS3).

6.1. Association delay

We measured the association delay of a device to the network via CPAN, in Table 1. As shown in this table, the average delay of association of our protocol is 43.26 ms. On the other hand, for solution WSN-SLAP the association delay is high. This difference is due to the use of fewer exchanged messages during the authentication and association phase between the device and CPAN. Finally,

compared to protocol WSN-SLAP, we can see that our authentication mechanism is optimal.

Table 1. Association delay

Protocol	Association delay (ms)
WSN-SLAP	620.234
AuthenIoT	43.26

6.2. Energy consumption

Optimizing energy consumption is one of the biggest challenges in the design of our protocol. Indeed, the security protocol should be optimized in order to maximize the lifetime of the objects and the network. In order to be able to prove the energy efficiency of our protocol, we will perform a theoretical estimate of the energy consumed by a device during the association phase of our protocol. In this study, we assume that the communication is completely reliable and that the association operation is performed without loss of packets. Energy can be calculated as follows:

$$E = P \times t \tag{6}$$

Where E is energy (in mJ), P is power (in mW), and t is time (in s). Energy E includes the energy consumed during the communication and the processing. Table 2 summarizes the results obtained. From this table, we can see that our protocol provides an efficient energy and consumes much less energy than approach WSN-SLAP. Indeed, approach WSN-SLAP uses asymmetric algorithms, which generally consume a lot of time and energy. Our protocol is optimized, it does not require a large number of exchanged messages and is based on robust and lightweight algorithms, which makes it very well suited to the requirements of IoT.

Table 2. Energy consumption

Association	AuthenIoT	WSN-SLAP
Number of messages	4	6
Execution time (ms)	41.32892	2953
Energy consumption (mJ)	38.29481	436.7

7. Conclusion

In this paper, we have proposed a light and efficient security protocol called AuthenIoT, which can be deployed on different IoT architecture and technologies and allows to protect their systems and their data via an efficient authentication mechanism. Our protocol provides the device authentication service to protect networks against spoofing attack. We have also created a mechanism to manage keys, which is a secure and flexible method of distributing pre-shared keys, which protects devices against internal spoofing attacks. We have improved the simple authentication service to mutual authentication between the device and the CPAN managing the network in order to be able to guarantee the legitimacy of the network. This method improves the mechanism of key generation and adds another mechanism, called a hidden broadcast key, for broadcast key. AuthenIoT has been simulated in the Network Simulator 3 (NS3). Simulation results show an improved performance compared to the related work.

References

[1] Atzori L., A. Iera, G.M., "The Internet of things: a survey," Comput. Netw., vol. 54, no. 15, pp. 2787-2805, 2010.

[2] Kardi A., R. Zagrouba R., "Attacks classification and security mechanisms in wireless sensor networks Advances in Science," Technology and Engineering Systems *Journal*, vol. 4, no. 6, pp. 229–243, 2019.

[3] Jha S., Nkenyereye, L., Prasad G.J., Yang E., "Mitigating and monitoring smart city using Internet of Things," *Computers, Materials Continua*, vol. 65, no. 2, pp. 1059–1079, 2020.

[4] Abbas S., Khan M.A., Falcon-Morales L.E., Rehman A., Saeed Y. et al., "Modelling, simulation and optimization of power plan energy sustainability for IoT enabled smart cities empowered with deep extreme leaning machine," *IEEE ACCESS*, vol. 8, no. 1, pp. 39982–39997, 2020.

[5] Alhajri R., Zagrouba R., Alhaidari F., "Survey for anomaly detection of IoT botnets using machine learning autoencoders," *International Journal of Applied Engineering Research*, vol. 14, no. 10, pp. 2417– 2242, 2019.

[6] Javaid U., Siang A. K., Aman M. N., Sikdar B., "Mitigating IoT device based DDoS attacks using blockchain," *in Proc. 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, pp. 71–76, 2018.

[7] Ting P. Y., Tsai J. L., Wu T. S., "Signcryption method suitable for low-power IoT devices in a wireless sensor network," *IEEE Systems Journal*, vol. 12, no. 3, pp. 2385–2394, 2018.

[8] Moinet A., Darties B., Baril J.L, "Blockchain based trust authentication for decentralized sensor networks," *Cryptography and Security*, vol. 1, pp. 1–6, 2017.

[9] Al-Naji F.H, and Zagrouba R., "A survey on continuous authentication methods in Internet of Things environment," *Computer Communications Journal*, vol. 163, pp. 109–133, 2020.

[10] Akyildiz I.F., Su W., Sankarasubramaniam Y., and Cayirci E.''A survey on Sensor networks", *IEEE Commun. Mag.* vol. 40, pp. 102–114, 2002.

[11] Yang S., Shiue Y., Su Z., Liu I., Liu C., "An Authentication Information Exchange Scheme in WSN for IoT Applications," *IEEE Access*, vol. 8, pp. 9728-9738, 2020.
[12] Hammi M.T., Livolant E, Bellot P., Serhrouchni A., Minet P., "A Lightweight Mutual Authentication Protocol for the IoT," *International Conference on Mobile and Wireless Technology*, pp. 3-12, 2018.
[13] A. Afzal A., Khan M.A, Abbas S., "Secure communication of IoT based devices using EPEB algorithm," *Journal of Information Assurance and Security*, vol. 13, no. 3, pp. 91–97, 2020.
[14] Kwon D.K, Yu S.J., Lee J.Y., Son S.H., Park Y.H.," WSN-SLAP: S.ecure and Lightweight Mutual Authentication Protocol for Wireless Sensor Networks," *Sensors*, vol. 21, no. 3, 2021.
[15] Khaldoun A., Gerard C., Alexandre G., Erwan L., Saoucene M., Pascale M., et al.," Cross-layering in an Industrial Wireless Sensor Network: Case Study of OCARI," *JNW*, vol. 4, no.6, pp. 411–420, 2009.
[16] Danny D., Andrew Y., "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no.2, pp. 198–208, 1983.
[17] Haller N., Metz M., Phil N., Straw M., "A one-time password system. Technical report", 1998.
[18] Raihi D., Bellare M., Hoornaert F., Naccache D., Ranen O., "HOTP : An HMACbased one-time password algorithm," *IETF, RFC 4226*, 2005.
[19] Dierks T., "The transport layer security (TLS) protocol," version 1.2. 2008.
[20] Buys B., "Estimating password cracking times. Technical report," Computer Secuity project, 2014.
[21] Cas Cremers C. "Scyther. Draft," 2014.
[22] Kaishan Wu., Ali R.L, Ali M., Ayub A., "A Review and State of Art of Internet of Things (IoT)," *Archives of Computational Methods in Engineering*, pp. 1-19, 2021.
[23] Laghari A.A., He H., Khan A., Kumar N., Kharel R.," Quality of experience framework for cloud computing (QoC)", *IEEE Access*, vol. 6, pp. 64876-64890, 2018.
[24] Jumani A., Laghari R.., "Review and State of Art of Fog Computing", *Archives of Computational Methods in Engineering*, pp. 1-13, 2021.
[25] Ali M., "Quality of experience assessment of calling services in social network", *ICT Express* vol. 7, no. 2, pp. 158-161, 2021.