An Ultra-Lightweight Authentication Scheme for Heterogeneous Wireless Sensor Networks in the Context of Internet of Things

Hamza Khemissa, Djamel Tandjaoui, Samia Bouzefrane

▶ **To cite this version:**

Hamza Khemissa, Djamel Tandjaoui, Samia Bouzefrane. An Ultra-Lightweight Authentication Scheme for Heterogeneous Wireless Sensor Networks in the Context of Internet of Things. International Conference on Mobile Secure and Programmable Networking (MSPN 2017), Jun 2017, Paris, France. 10.1007/978-3-319-67807-8_4 . hal-02425154

HAL Id: hal-02425154
https://hal.science/hal-02425154

Submitted on 29 Dec 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

An ultra-lightweight authentication scheme for heterogeneous wireless sensor networks in the context of Internet of Things

Hamza Khemissa [1,2(✉)], Djamel Tandjaoui [1], and Samia Bouzefrane [3]

[1] Computer Security Division, CERIST: Research Center on Scientific and Technical Information, Algiers, Algeria
[2] LSI, USTHB: University of Sciences and Technology Houari Boumediene, Algiers, Algeria
[3] CEDRIC Lab, CNAM: National Conservatory of Arts and Crafts, Paris, France
{hkhemissa,dtandjaoui}@cerist.dz
h.khemissa@usthb.dz
samia.bouzefrane@lecnam.net

Abstract. The Internet of Things (IoT) is in a continuous development, the basic notion of IoT is that each object within the global network is accessible and interconnected. In such an environment, Wireless Sensor Networks play a crucial role, since they support different applications domains. Nevertheless, security issues are the major obstacle for their deployment. Among these issues, authentication of the different interconnected entities and exchanged data confidentiality. In this paper, we propose a new ultra-lightweight authentication scheme for heterogeneous wireless sensor networks in the context of IoT. This scheme allows both of the sensor and the user to authenticate each other in order to secure the communication. The proposed scheme uses only nonces, exclusive-or, concatenation operations to achieve mutual authentication. Moreover, it terminates with a session key agreement between the sensor node and the user. To assess our scheme, we carry out a performance and security analysis. The obtained results show that the proposed scheme provides authentication with low energy consumption, and ensures a resistance against different types of attacks.

Keywords: Internet of Things · Wireless Sensor Networks · Identity · Authentication · Session key agreement

1 Introduction

The Internet of Things (IoT) is designed as a network of highly heterogeneous connected devices (things) that have locatable, addressable, and readable counterparts on the Internet [11]. It includes several kinds of objects, and different in terms of capability and functionality such as Radio-Frequency IDentification

(RFID) tags, sensors, smartphones, wearable, etc. These heterogeneous objects interact to reach common goals [2] [11] [16].

IoT deployment will open doors to a multitude of application domains, such as healthcare, military, logistics, environmental monitoring, and many others [2]. Wireless Sensor Networks (WSN) are considered as one of actual and most effective IoT applications network. Nowadays, we talk about heterogeneous WSNs since sensor networks can be built with different types of nodes, and some more computational and energy capabilities than others.

The most of communications are wireless in the IoT, which have the risk of eavesdropping. Thus, IoT is vulnerable to different types of attacks. Involved devices in the IoT have also low capabilities in terms of energy and computation. Hence, they cannot support the implementation of complex security schemes [2]. Security issues are the major obstacle for several IoT applications. Among these issues, authentication is an important concept that allows to verify the identity of each connected objects. Also, data integrity and confidentiality are required to secure communications [2] [16].

In the literature, there are five basic authentication models for WSNs [21]. They need four messages to achieve authentication. In four of them, the user initiates the authentication scheme by firstly contacting the gateway node, then the sensor node. When developing our proposed ultra-lightweight authentication scheme for heterogeneous WSNs, we use the fifth authentication model, such as it is the only one that initiates the authentication scheme by firstly contacting the specific sensor. In our network architecture (see Figure 1), a sensor node is the initiator of the authentication. Thus, it has to initiate the authentication scheme with the user directly through the Internet and does not need to first connect with the gateway node.

In this paper, we propose an ultra-lightweight authentication scheme for heterogeneous WSNs in the context of IoT. This scheme authenticates both of a sensor node and the user, and establishes a secure channel between the sensor node and the user. The proposed scheme uses only nonces, exclusive-or, concatenation operations to achieve mutual authentication. To assess our proposed scheme, both in terms of security properties and energy savings, we proceed with a security and a performance analysis. The obtained results show that is resistant against several attacks, and it provides authentication with low energy consumption.

The remainder of the paper is organized as follows. In Section 2, related work on authentication in the context of IoT are presented. Section 3 presents in details the network architecture, used notations, and the proposed authentication scheme. In section 4 and 5, we continue with a security and performance analysis of the proposed scheme. Finally, section 6 concludes the paper and provides future works.

2 Related work

During the past few years, the research community focuses on proposing new security protocols adapted to the constrained environment of the IoT. In the related work discussion, we mainly discuss several proposed authentication schemes in the context of IoT. Among critical security issues in the IoT, Authentication is an important aspect used in different applications domains [2] [16].

Traditional authentication schemes usually interacts with centralized servers and identity providers [4]. These interactions generally require a high energy and computation capabilities. Nevertheless, most objects that constitute the IoT are limited in these resources. Many research works aim to propose lightweight and ultra-lightweight schemes adapted to IoT environment limits. Several research works on authentication in the context of IoT are cited in [2] [16]. Recent proposed authentication schemes in the context of IoT can be divided into two classes, namely: authentication with certification, and certificateless authentication.

In the first class, authentication is achieved by using digital certificates, such as each object has its digital certificate. Among these protocols, DTLS (Datagram Transport Layer Security) [14] authentication handshake has been proposed for the IoT [8]. This authentication scheme ensures a secure authentication between the two involved objects. However, its high consumption of energy caused by asymmetric encryption based RSA and the use of PKI certificates exchanges constitute its main drawbacks. For this reason, Elliptic Curve Cryptography (ECC) has raised as an interesting approach compared to RSA based algorithms. Indeed, for the same level of security, it consumes less energy and uses less key size for the same level of security [17].
In order to reduce the energy cost of the authentication process, authors in [12] [13] have proposed an authentication protocol for WSNs in distributed IoT applications. This scheme uses ECC based implicit certificate [1]. The analysis shows that it offers an authentication with less energy consumption and computation overhead.

In the second class, authentication schemes do not need certification. They are based on cryptographic operations such as exclusive-or operation (Xor), concatenation operation, hash functions, and other symmetric cryptography functions. Thus, this class of authentication schemes is known for its high energy saving.
In 2013, authors in [19] have proposed a user authentication and key agreement scheme based on the IoT notion for heterogeneous ad hoc WSNs. This scheme uses only symmetric cryptographic operations between a remote user, a gateway, and a sensor node. It terminates by a session key establishment that secures communication between the remote user and the sensor node.
In 2014, Farash et al. [5] reviewed this scheme, and they showed some security weaknesses. In order to overcome these weaknesses, they proposed a new and an efficient user authentication and key agreement scheme. The results of security

analysis confirm the security properties of the proposed scheme.
In 2016, authors in [7] have proposed a new lightweight authentication for heterogeneous WSNs in the context of IoT. The scheme uses nonces and keyed-hash message authentication (HMAC) [9].In addition, the HMAC computation is based on sensor node identity without sending the identity on the clear message. The analyses prove that the proposed scheme is classified as lightweight since it provides authentication with low energy cost.

Tewari et al. [18] have proposed an ultralightweight authentication scheme that uses only bitwise operation for IoT devices using RFID tags. The analysis of the scheme showed that is resistant against several attacks such as desynchronization, secret disclosure and traceability attacks. Nevertheless, authors in [15] have showed that is not resistant against the mentioned attacks. Furthermore, they presented a passive attack that retrieves all secret parameters of the tag by only eavesdropping a session between the legitimate reader and the target tag in a very short time.

Recently, authors in [6] have proposed a lightweight anonymous authentication protocol for securing real-time application data access in WSNs. The security analysis of this scheme showed that it provides several security features with a high security level. However, the sensor identity is not protected since it is sent on clear in the authentication phase. Based on the performance analysis of the scheme, it has low communication and computation costs. Consequently, it is suitable to be applied in resource constrained environments.

In this work, we propose a new utlra-lightweight authentication scheme with a high level of security and very low energy cost. This scheme is adaptable to each object that can be involved on heterogeneous WSNs in the context of IoT. It provides mutual authentication and key establishment to maintain a secure communication channel for confidential exchanges.

3 The proposed scheme

In this section, we present the proposed authentication scheme that aims to provide a mutual authentication between a sensor node and a user. This latter achieves authentication with low resources consumption. Firstly, we describe the network architecture and the used notations. Secondly, we define in details the functioning of the proposed authentication scheme.

3.1 Network architecture

The network architecture is mainly composed of: the sensor nodes, the gateway node, and the user (see Figure 1). The used authentication model enables a direct transmission of collected data from a sensor node to the mobile user after a successful mutual authentication between a sensor node and the user.

According to the network architecture, we make some assumptions:

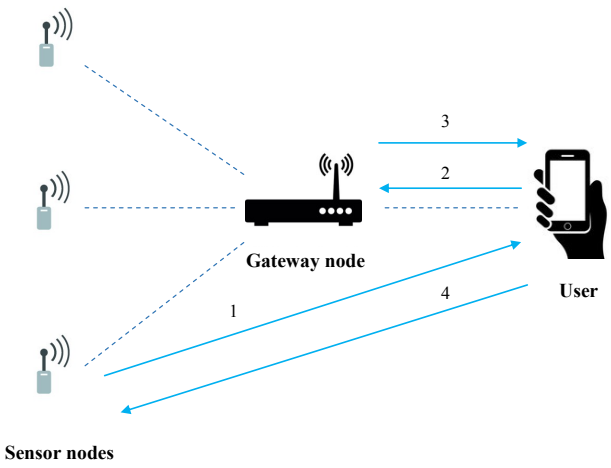

Fig. 1. Network architecture

- Objects can be divided into two categories: Sensor nodes are constrained on computational and energy capabilities. The gateway node and the user are non-constrained since they have more computational and energy resources.

- Each sensor has an identity Id_i and a masked identity $MSId_i$, it has the capacity to perform symmetric encryption. The gateway node and the user are able to perform asymmetric encryption to secure data transmission outside the WSN.

3.2 Notations

The notations used in the proposed scheme are defined in Table 1.

Table 1. Used Notations

Notation	Description
$\|$	Concatenation
$\oplus$	Exclusive-or operation (Xor)
N	Nonce value of the sensor node
M	First nonce value of the user
L	Nonce value of the gateway node
P	Second nonce value of the user
H()	A one way hash function
Enc(N,X_i)	AES-128 encryption of the value N using the secret key X_i
F(N)	If (N != 16 bytes) : The Function F applies an hash function h() that returns 16 bytes

3.3 Functioning

The proposed authentication scheme provides a mutual authentication and a session key agreement between a sensor node and a user that aims to collect data from the WSN. The scheme is divided into three phases:

- The registration phase, where the sensor nodes must first be registered in gateway node. Then, a registration part between the gateway and the user.
- The authentication phase between the sensor nodes, the gateway, and the user in order to achieve mutual authentication.
- The key establishment, where a session key is established between each sensor node and the user.

In the following, we will present each phase in details.

1) Registration phase

The registration phase between the sensor nodes, the gateway node, and the mobile user is the first phase of the proposed scheme. This phase is divided into two parts. The first registration part is between the sensor node and the gateway node, we assume that the communication channel has been previously secured. The second registration part is between the gateway node and the user (see Figure 2).

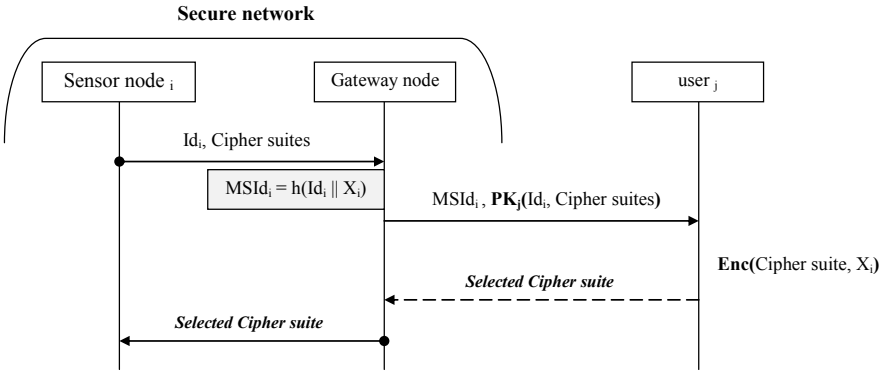

Fig. 2. Registration phase

First, the sensor node sends its identity Id_i and a list of supported cipher suites to the network gateway node through a secure channel. Once the gateway node receives the message, it selects the used cipher suite, and calculates the masked identity of the sensor node $MSId_i$ using the sensor identity Id_i and its secret key X_i. Second, it sends a message containing the masked identity of the

sensor node, and the encryption of both the identity of the sensor node Id_i and the selected cipher suite by the public key of the user PK_j. (We assume that the gateway node knows the secret key of the sensor node and the public key of the user during the pre-deployment of the network).

As a response, the user sends an encrypted message *Selected Cipher suite* using the secret key of the sensor. This message contains the selected cipher suite. Finally, the gateway node transmits the *Selected Cipher suite* message to the sensor node. The sensor node receives, decrypts the message, and the registration phase terminates successfully.

Once the registration phase terminates, both of the gateway node and the user store the security related information in a binding table (see Table 2).

Table 2. Security Related Information

Node	Cipher suite	Masked Identity: $MSId_i$=h(Id_i ‖X$_i$)
Id_1	Cipher1 & X_1	$MSId_1$
Id_2	Cipher2 & X_2	$MSId_2$
Id_3	Cipher3 & X_3	...

2) Authentication phase

The authentication phase aims to mutually authenticate both of the sensor nodes and the user. The authentication process must be executed to ensure a secure communication between each sensor node and the user. Our proposed authentication scheme is as follows (see Figure 3):

a) The sensor node generates a random nonce N on 8 bytes, calculates the value Z=(N ‖ Id_i) ⊕ X_i, devises the value Z into two parts of 8 bytes: Z1 and Z2, applies a Xor between the two parts (Z1 ⊕ Z2), and puts the result on Z. Then, it sends a message composed of the masked identity of the sensor $MSId_i$, the generated nonce N, and the value Z to the user. The value Z will be used by the user to check the message.

b) Upon receiving the message by the user, the message is verified by computing the value Z, and checking whether the received Z equal the computed value. If not equal, it is an authentication failure (F1), else the user generates a random nonce M on 8 bytes, calculates the value W=(M ‖ Id_i) ⊕ X_i, devises the value W into two parts of 8 bytes: W1 and W2, applies a Xor between the two parts (W1 ⊕ W2), and puts the result on W. Then, it sends a message composed of the masked identity of the sensor $MSId_i$, the nonce N, the generated nonce M, and the value W to the user. The value W will be used by the gateway node to check the message.

c) When the gateway node receives the message, it also verifies the message by calculating the value W, and checking whether the received W equal the computed value. If not equal, it is an authentication failure (F2), else the gateway

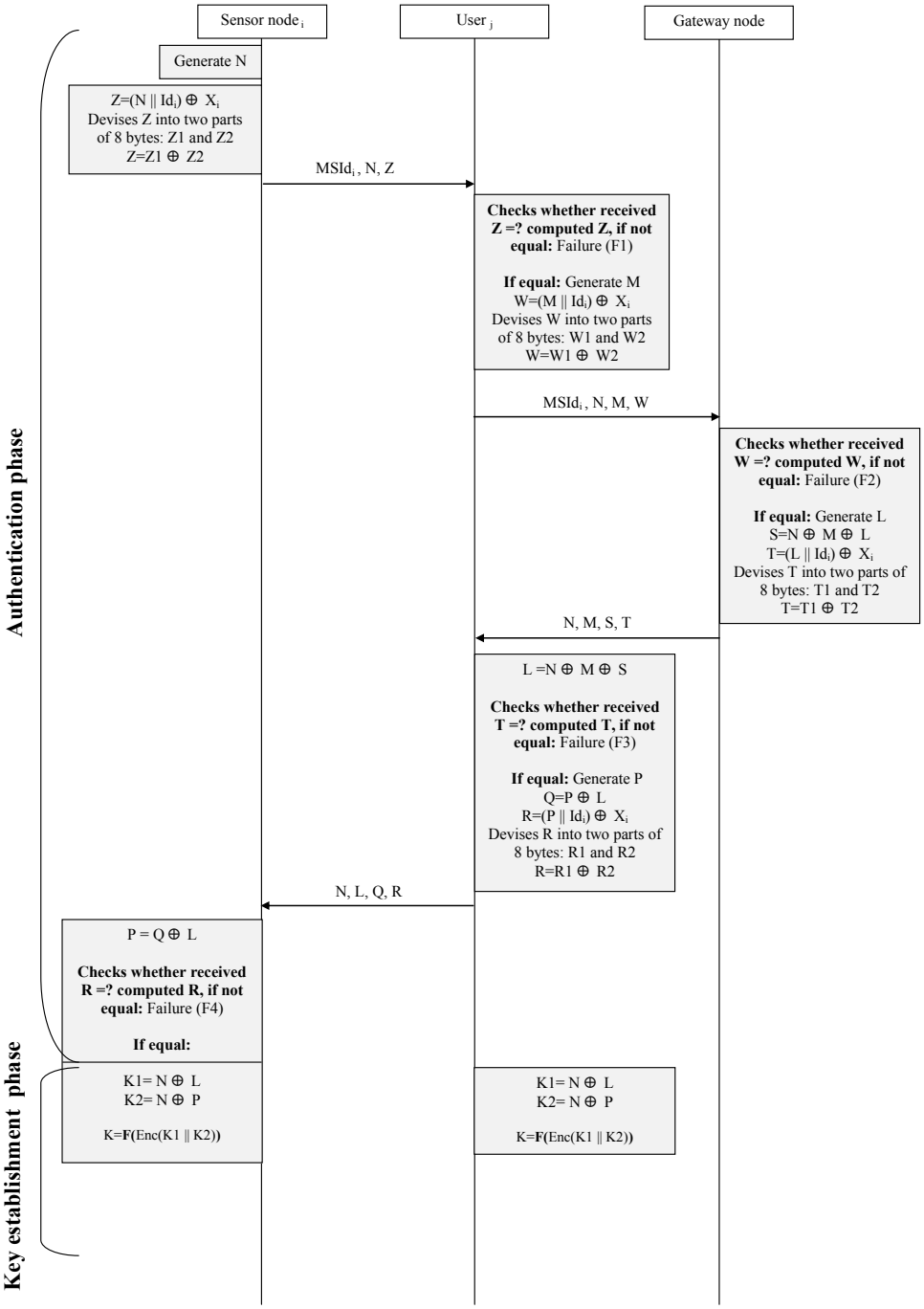

Fig. 3. Authentication scheme

node generates a random nonce L on 8 bytes, calculates the value S=N $\oplus$ M $\oplus$ L, calculates the T=(L $\|$ Id_i) $\oplus$ X_i, devises the value T into two parts of 8 bytes: T1 and T2, applies a Xor between the two parts (T1 $\oplus$ T2), and puts the result on T. Then, it sends a message composed of the nonce N, the nonce M, and the values S and T to the user. The value T will be used by the user to check the message.

d) Upon receiving the message by the user, it computes the value L=N $\oplus$ M $\oplus$ S, and verifies the message by checking whether the received T equal the computed value. If not equal, it is an authentication failure (F3), else the user generates a random nonce P, calculates the value Q=P $\oplus$ L, computes the value R=(P $\|$ Id_i) $\oplus$ X_i, devises the value R into two parts of 8 bytes: R1 and R2, applies a Xor between the two parts (R1 $\oplus$ R2), and puts the result on R. Then, it sends a message composed of the nonce N, the nonce L, and the values Q and R to the sensor node. The value R will be used by the sensor node to check the message.

e) When the sensor node receives the message, it computes the value P=Q $\oplus$ L, and verifies the message by checking whether the received R equal the computed value. If not equal, it is an authentication failure (F4), else mutual authentication between objects terminates successfully.

3) Key establishment phase

After a successful authentication phase, a shared symmetric key K is established to secure the communication between the sensor node and the user. This key is calculated by a personalized function as: K=F(Enc(K1 $\|$ K2,X_i)). First, the values K1 and K2 are calculated by applying respectively a Xor of the value N with the nonces L and P. Second, the concatenation of the two values K1 and K2, and apply an encryption with the associated secret key of the sensor node X_i. Thus, the key establishment phase terminates.

4 Security analysis of the proposed scheme

In order to show the security efficiency of the proposed authentication scheme, we conduct a security analysis of the scheme. Our proposed scheme offers a resistance to several possible attacks. We are interested especially to:

- *Replay attack:*

If an attacker intercepts a previous exchanged message in the authentication phase, and tries to replay it in order to impersonate the sensor node, the user, or the gateway node, the message will be rejected and he cannot successfully impersonate the sensor node, the user, or the gateway node because new nonces are generated for each authentication to provide mutual authentication.

- *Impersonation attacks:*

First, an attacker cannot impersonate a sensor node since his identity is masked by the value $MSId_i$. Second, it cannot also impersonate the user or the

gateway node without computing the value that checks the exchanged message using the sensor identity Id_i and the secret key X_i.

- *Denial-of-service attack:*

This attack is extremely dangerous in a resource constrained IoT environment. The Denial-of-service (DoS) attack has different types of attacks e.g. Jamming, Flooding, Tampering, etc. [20]. We threat the case of Flooding attack, since it can affect the proposed authentication scheme. The Flooding attack is not possible since each exchange in the authentication phase requests a response message that indicates the rejection or the acceptance of the received message, and ensures that is not a DoS attack. Furthermore, the proposed scheme uses random nonces, which are accepted only once in the authentication phase. Thus, it provides resistance against DoS attacks.

The proposed authentication scheme provides also advanced features that enhance security such as:

- *Mutual authentication:*

As a result of the authentication phase, both of the authenticity of the sensor node and the user is proven. This process is called mutual authentication. Therefore, both of the sensor node and the user are sure of the identity of each other.

- *Session key establishment:*

After a successful authentication, a shared secret key is established between the sensor node and the user. This key is used as a session key to ensure a secure communication channel.

- *Data integrity:*

In the authentication phase of the proposed scheme, the integrity of a message is verified by the check of the computed value sent with the message. Thus, we are sure that transmitted data are not altered, and the integrity of exchanged messages is ensured.

- *Sensor identity protection:*

In order to disallow the revelation of the sensor identity Id_i, a masked identity $MSId_i$ is calculated for each sensor node. This value will be also known by the gateway node and the user.

- *Synchronization independence:*

In the proposed authentication scheme, we use random nonces to guarantee the freshness of messages. Thus, the proposed scheme does not require the use of timestamps to synchronize between involved objects. Therefore, the synchronization independence enhances the security of the proposed scheme.

- *Extensibility and scalability:*

The proposed authentication scheme allows new sensor nodes to be integrated into the network system through the registration phase. Thus, a new sensor node is registered into the the gateway node and the user, and the security related information table is updated with its identity, masked identity, and used cipher

suite.

As a result of security analysis, the proposed scheme is suitable for insecure IoT environments in which an attacker can eavesdrop communications between involved objects.

5 Performance analysis of the proposed scheme

In this section, we provide a performance analysis of the proposed authentication scheme. We focus on the energy evaluation of the sensor node as a constrained object. We use a TelosB sensor node equipped with a CC2420 radio. This latter typically runs on two AA batteries, which combine about 18500 J. To estimate the energy consumption of the proposed scheme, we compute the energy required for the execution of the cryptographic primitives along with the energy required for communication (transmission and reception of data, with 12 bytes of protocol headers).

Authors in [3], have presented an energy evaluation of wireless sensor nodes regarding the communication cost. In addition, the cost of the different used symmetric cryptography functions has been evaluated in [10]. Table 3 summarizes the deduced values, which are used as an energy model.

Table 3. Estimated energy costs on the sensor node [3] [10]

Operation	Cost
Transmission of 1 byte	5.76 μJ
Reception of 1 byte	6.48 μJ
AES-128 encryption of 16 bytes	42.88 μJ

Based on the estimated values, we evaluate the energy consumption of the proposed authentication scheme in the authentication phase and the key establishment phase. Furthermore, we study the different cases of an authentication failure, and we evaluate the energy consumption in the authentication failure cases: F1, F2, F3 and F4 as shown in Table 4.

As described in the proposed scheme, a sensor node has to send its masked identity (20 bytes), the generated nonce value (8 bytes), and the computed value (8 bytes). Thus, the length of the transmitted message is 48 bytes (20 bytes + 8 bytes + 8 bytes + 12 bytes of protocol headers) which requires 276.48 μJ to be transmitted. As a response from the user, the sensor receives a message of 44 bytes (8bytes + 8 bytes + 8 bytes + 8 bytes + 12 bytes of protocol headers) which requires 285.12 μJ to be received. Hence, the total energy cost of the authentication phase is equal to 561.6 μJ.

In the key establishment phase, an encryption of the concatenation of the two values K1 and K2 requires about 42.88 μJ (result of encryption on 16 bytes), and

applying the function F if necessary (In our case, the result of the computation of the shared key K is on 16 bytes, we do not apply the function F). Therefore, the total energy cost of the key establishment phase is 42.88 μJ.

The total cost of the the scheme is the cost of the authentication phase plus the cost of the establishment phase: 604.48 μJ. A very low energy cost proving that the proposed scheme is ultra-lightweight and suitable to be applied in a resource constrained IoT environment.

Table 4. Analysis of the authentication scheme

Case of authentication	Energy consumption	Number of sent messages	Number of received messages
F1	276.48 μJ	1	0
F2	276.48 μJ	1	0
F3	276.48 μJ	1	0
F4	561.6 μJ	1	1
Successful authentication	604.48 μJ	1	1

As a result from the evaluation of different scenarios of the authentication scheme (see Figure 4), we deduce that the proposed scheme also saves energy in the different cases of an authentication failure. The energy consumption in the authentication failures F1, F2, and F3 is just 276.48 μJ, and 561.6 μJ in the authentication failure F4. Consequently, the obtained results enhance the scheme performance.

The energy cost of the proposed scheme is very interesting compared to our previously proposed lightweight authentication scheme in [7] that consumes 883.98 μJ (see Figure 5).

6 Conclusion

In this paper, we have proposed a new ultra-lightweight authentication scheme for WSN applications in the context of IoT. This scheme uses only nonces, exclusive-or, concatenation operations in the authentication phase. Besides, it uses the concept of masked identity to protect the sensor identity, and only one symmetric encryption in the key establishment phase. The proposed scheme has low costs of communication and computation with a high level of security, and saves energy in the different cases of an authentication failure. Thus, it is suitable to be deployed in a resource constrained environment.

In order to obtain more accurate analysis study especially on memory consumption and execution time, we aim to simulate the proposed authentication scheme using Cooja simulator of Contiki OS and to test it in a real deployment.

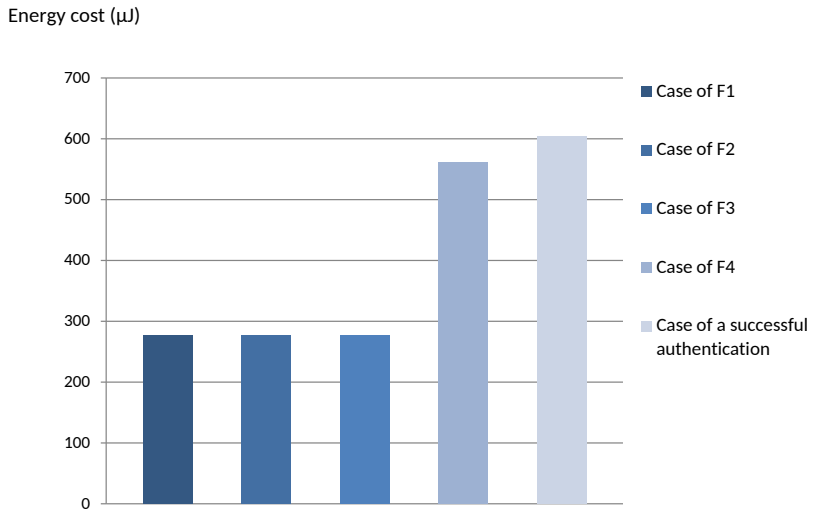

Fig. 4. Energy cost analysis of the proposed authentication scheme

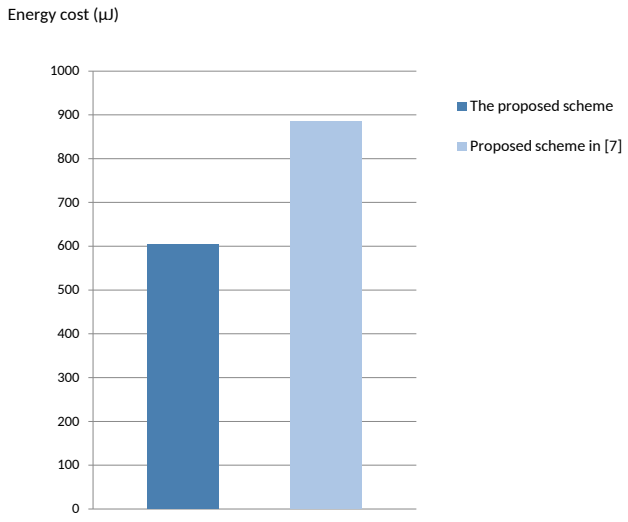

Fig. 5. Energy cost comparison of the proposed authentication scheme

References

1. SEC4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV), version 0.97. www.secg.org (August 2013)
2. Atzori, L., Iera, A., Morabito, G.: The internet of things: A survey. Computer networks 54(15), 2787–2805 (2010)
3. De Meulenaer, G., Gosset, F., Standaert, O.X., Pereira, O.: On the energy cost of communication and cryptography in wireless sensor networks. In: Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing,. pp. 580–585. IEEE (2008)
4. El Maliki, T., Seigneur, J.M.: A survey of user-centric identity management technologies. In: Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007. The International Conference on. pp. 12–17. IEEE (2007)
5. 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)
6. Gope, P., Hwang, T.: A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. IEEE Transactions on Industrial Electronics (2016)
7. Khemissa, H., Tandjaoui, D.: A novel lightweight authentication scheme for heterogeneous wireless sensor networks in the context of internet of things. In: Wireless Telecommunications Symposium (WTS), 2016. pp. 1–6. IEEE (2016)
8. Kothmayr, T., Schmitt, C., Hu, W., Brünig, M., Carle, G.: Dtls based security and two-way authentication for the internet of things. Ad Hoc Networks 11(8), 2710–2723 (2013)
9. Krawczyk, H., Canetti, R., Bellare, M.: Hmac: Keyed-hashing for message authentication (1997)
10. Lee, J., Kapitanova, K., Son, S.H.: The price of security in wireless sensor networks. Computer Networks 54(17), 2967–2978 (2010)
11. Nguyen, K.T., Laurent, M., Oualha, N.: Survey on secure communication protocols for the internet of things. Ad Hoc Networks 32, 17–31 (2015)
12. Porambage, P., Schmitt, C., Kumar, P., Gurtov, A., Ylianttila, M.: Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications. International Journal of Distributed Sensor Networks 2014 (2014)
13. Porambage, P., Schmitt, C., Kumar, P., Gurtov, A., Ylianttila, M.: Two-phase authentication protocol for wireless sensor networks in distributed iot applications. In: Wireless Communications and Networking Conference (WCNC), 2014 IEEE. pp. 2728–2733. IEEE (2014)
14. Rescorla, E., Modadugu, N.: Datagram transport layer security version 1.2 (2012)
15. Safkhani, M., Bagheri, N.: Passive secret disclosure attack on an ultralightweight authentication protocol for internet of things. Tech. rep., Cryptology ePrint Archive, Report 2016/838, 2016. http://eprint. iacr. org/2016/838
16. Sicari, S., Rizzardi, A., Grieco, L., Coen-Porisini, A.: Security, privacy and trust in internet of things: The road ahead. Computer Networks 76, 146–164 (2015)
17. Szczechowiak, P., Oliveira, L.B., Scott, M., Collier, M., Dahab, R.: Nanoecc: Testing the limits of elliptic curve cryptography in sensor networks. In: Wireless sensor networks, pp. 305–320. Springer (2008)
18. Tewari, A., Gupta, B.: Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for iot devices using rfid tags. The Journal of Supercomputing pp. 1–18 (2016)

19. 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)
20. Wood, A.D., Stankovic, J., et al.: Denial of service in sensor networks. Computer 35(10), 54–62 (2002)
21. Xue, K., Ma, C., Hong, P., Ding, R.: A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. Journal of Network and Computer Applications 36(1), 316–323 (2013)