A Novel Lightweight Authentication Scheme for heterogeneous Wireless Sensor Networks in the context of Internet of Things

Hamza Khemissa*, Djamel Tandjaoui†
*†Security Division, CERIST: Research Center on Scientific and Technical Information
*LSI, USTHB: University of Sciences and Technology Houari Boumediene Algiers, Algeria
Email: {hkhemissa, dtandjaoui}@cerist.dz, h.khemissa@usthb.dz

***Abstract*—The evolution of Internet of Things (IoT) is changing traditional perceptions of the current Internet towards a vision of smart objects interacting with each other. Wireless Sensor Networks play an important role and support different applications domains in the IoT environment. However, security issues are the major obstacle for their deployment. Among these issues, authentication of the different interconnected entities. In this paper, we are interested to the case of the interconnection of a sensor node with a remote user. We propose a new lightweight authentication scheme adapted to the resource constrained environment. This scheme allows both of the sensor and the remote user to authenticate each other in order to secure the communication. Our scheme uses nonces, exclusive-or operations, and Keyed-Hash message authentication to check the integrity of the different exchanges. The proposed method stands out in that it provides authentication with less energy consumption, and it terminates with a session key agreement between the sensor node and the remote user. To assess our scheme, we carry out a performance and security analysis. The obtained results show that our scheme saves energy, and provides a resistance against different types of attacks.**

***Keywords*—Internet of Things; Wireless Sensor Networks; Identity; Authentication; Session key agreement.**

I. INTRODUCTION

In the last few years, Internet of Things (IoT) is rapidly gaining ground in the area of wireless communications and networking. The basic idea is the interconnection of an heterogeneous objects such as Radio-Frequency IDentification (RFID) tags, sensors, mobile phones, wearable, etc. These heterogeneous objects interact to reach common goals [1] [2]. Each connected object has a locatable, addressable, and readable counterpart on the Internet. IoT deployment will open doors to a huge number of applications. Wireless Sensor Networks (WSN) are considered as one of actual and most effective IoT applications network. They cover a wide application domain for the IoT such as e-health, military, industrial applications, etc.

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 (e.g. gateway nodes). The heterogeneity of a WSN with the possibility of a direct communication with each other and with the rest of the world (e.g. ad hoc) are two important notions of IoT.

IoT is extremely vulnerable to different attacks. This vulnerability is due to the fact that most of the communications are wireless, which have the risk of eavesdropping. In addition, the characteristics of most IoT components that have low capabilities in terms of both energy and computing resources. Therefore, they cannot support the implementation of complex security schemes [2]. The major security problems concern authentication and data integrity [1]. For instance, authentication in the context of the IoT is an important concept that allows verifying the authenticity of each entity.

According to Xue et al. [3] there are five basic authentication models for WSNs. Each of the five presented authentication models needs four messages to complete the authentication. In four of the five models, the user initiates the authentication scheme with the sensor node, by firstly contacting the gateway node.

When developing our novel lightweight mutual authentication and key agreement scheme for heterogeneous WSNs, we focused on the resource constrained architecture of WSNs and security requirements. We use the fifth authentication model. This model is the only one which initiates the authentication scheme by firstly contacting the specific object. In our network architecture (see figure 1), a sensor node has to initiate the authentication scheme with the remote user without firstly contacting the gateway node.

In this paper, we propose a novel lightweight authentication scheme for heterogeneous WSNs in the context of IoT. The scheme authenticates each object and establishes a secure channel between the sensor node and the remote user. Our scheme uses nonces and keyed-hash message authentication (HMAC) [4]. It provides authentication with less energy consumption, protects the sensor node identity from disclosure, and terminates with a session key agreement between a sensor node and a remote user. The scheme provides also mutual authentication and a high security level against several attacks.

The remainder of the paper is organized as follows. In Section II, related work on authentication in the context of IoT are presented. Section III presents in details the network architecture, and our proposed authentication scheme. In section IV and V, we continue with a security and performance analysis of the proposed scheme. Section VI presents a variant of our scheme based on a lightweight PKI (Public Key Infrastructure). Finally, section VII concludes the paper and provides future works.

978-1-5090-0314-3/16/$31.00

II. Related work

The research community is currently focusing on proposing new security protocols that take into consideration the constrained environment of the IoT. In the related work discussion, we mainly discuss authentication protocols in the context of IoT.

Authentication is an important mechanism used since the emergence of the Internet. The traditional authentication on local networks or on the Internet usually interacts with centralized authentication servers and identity providers [5]. These interactions have generally a high energy cost and require certain capability on computation. However, different objects that constitute the context of IoT are limited on these resources. Many research works aim to propose effective solutions in order to deploy authentication protocols adapted to IoT environment limits. Different network architectures are based on IoT notions and need the deployment of an authentication scheme to secure communications. Several research works on authentication deployed in different network architectures which constitute the context of IoT are cited in [1] [2].

Recent works on authentication protocols in the IoT environment can be divided into two classes namely: authentication with certification, and certificateless authentication.

In the first class, authentication is achieved on the basis of digital certificates where each object must have its own digital certificate. Among these protocols, DTLS (Datagram Transport Layer Security) [6] authentication handshake has been proposed for the IoT [7]. This protocol offers an authentication between the different objects. However, its high consumption of energy caused by asymmetric encryption based RSA and the 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. In fact, it is more energy saving and less key size for the same level of security [8].
In order to reduce the energy cost of the authentication process, authors in [9] [10] have proposed an authentication protocol for WSNs in distributed IoT applications using ECC based implicit certificate [11]. It offers a less energy consumption and computation overhead.

In the second class, authentication protocols do not need certification. It uses cryptographic operations such as exclusive-or operation (Xor), hash functions, and symmetric cryptography.
This class is often known for its high energy saving. For this purpose, authors in [12] [13] have proposed a user authentication and key agreement scheme based on the IoT notion for heterogeneous ad hoc WSNs. It uses only cryptographic operations between a remote user, a gateway, and a sensor node. It terminates by an establishment of a secret shared key linking the remote user and the sensor node.
Recently, authors in [14] proposed a new authentication scheme. The scheme introduces a new method to securely send messages in the authentication phase. The exchanged messages are sent protected by a HMAC. 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 less energy consumption.

In this work, we propose a new certificateless authentication scheme with a very low energy consumption and a high level of security, adaptable to each object that can be involved on heterogeneous WSNs in the context of IoT. The scheme provides mutual authentication and key establishment to maintain a secure communication channel.

III. The proposed scheme

In this section, we present our authentication scheme that aims to authenticate both of the sensor node and the remote user. The scheme ensures mutual authentication with minimal resource consumption. At first, we describe the network architecture and the used notations. Then, we define in details the functioning of our authentication scheme.

A. Network architecture

The network architecture is mainly composed of: the sensor nodes, the gateway node, and the remote user (see figure 1). The proposed communication system enables collected data from a sensor node to be transmitted directly to the mobile remote user after a successful mutual authentication between a sensor node and the remote user.

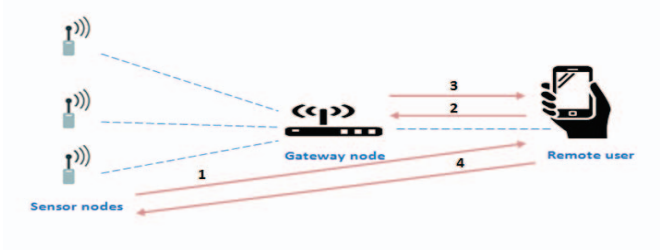

Fig. 1. Network Architecture

According to the network architecture, we make some assumptions about involved devices:

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

- Each sensor has an identity Id_i and a masked identity $MSId_i$, it has the capacity to perform symmetric encryption, and at least one asymmetric encryption. The gateway node and the remote user are able to perform classical PKI to secure data transmission outside the WSN since they are non-constrained.

B. Notations

For reader's convenience, the notations used in our scheme are defined in Table I.

C. Functioning

The proposed authentication scheme provides a mutual authentication between a sensor node and the remote user of the WSN application. The scheme is divided into three phases:

- The registration phase, where the sensor nodes must first be registered in gateway node, and then in the remote user.

TABLE I. USED NOTATIONS

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

- The authentication phase between each sensor node, the gateway, and the remote user in order to authenticate each other.
- The shared key establishment, where a session key is established between the sensor node and the remote 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 remote user is important in the functioning of the proposed scheme. It is divided into two parts. The first registration part is between the sensor node and the gateway node. The second registration part is between the gateway node and the remote user (See Figure 2).

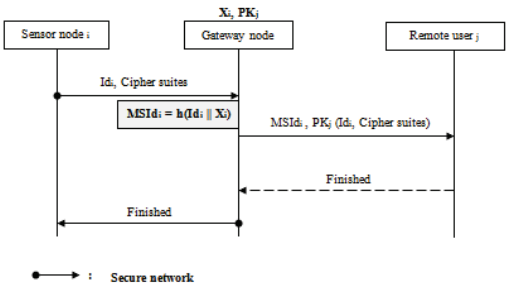

Fig. 2. Registration phase

The sensor node sends its identity Id_i and a list of the supported cipher suites to the network gateway node through a secure channel (we assume that the communication between the sensor node and the gateway node is previously secured). The gateway node 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. Then, it sends a message containing the masked identity of the sensor node $MSId_i$, plus the encryption of both the identity of the sensor node Id_i and the selected cipher suite by the public key of the remote user PK_j (During the pre-deployment of the network, the gateway node knows the secret key of the sensor node, as well as the public key of the remote user).
As a response, the remote user sends an encrypted message *Finished* with the secret key of the sensor containing the selected cipher suite. Finally, the gateway node transmits the *Finished* message to the sensor node.

Upon receiving the message by the sensor node the registration phase terminates successfully.
At the end of the registration phase, both of the gateway node and the remote user store the security related information in a binding table as shown in Table II.

TABLE II. 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 remote user. Each sensor node that wants to communicate with the remote user must execute the authentication process. Our authentication scheme is as follows (See figure 3):

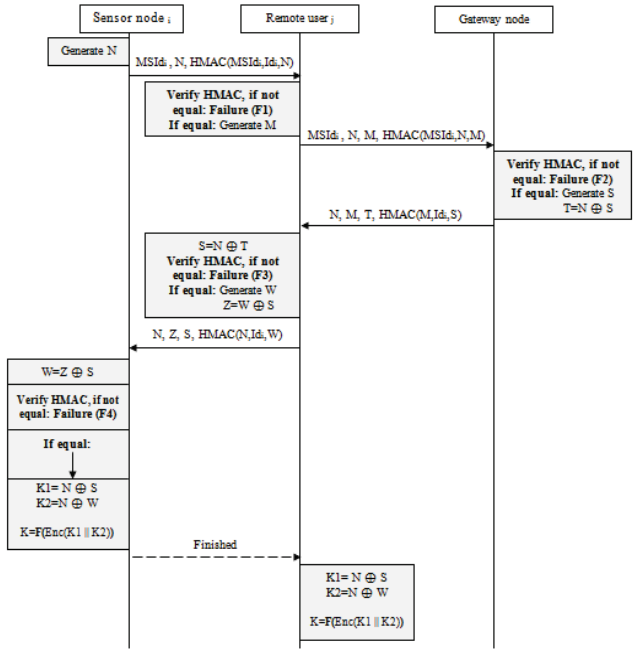

Fig. 3. Authentication scheme

a) The sensor node generates a random nonce N on 8 bytes and sends a message composed of the generated nonce, its masked identity $MSId_i$, and a HMAC ($MSId_i$, N, Id_i) to the remote user.

b) Upon receiving the message by the remote user, the message is verified by computing the associated HMAC. If the check is successful, the remote user also generates a random nonce M on 8 bytes, and transmits to the gateway node a message composed by the masked identity of the sensor node $MSId_i$, the received nonce N, the nonce M, and a HMAC ($MSId_i$, N, M).

c) When the gateway node receives this message, it also verifies the message by calculating the associated HMAC. If the check is successful, the gateway node generates a random nonce S on 8 bytes, and applies a XOR with the received value N: (T = N $\oplus$ S). The gateway node, in turn, sends to the remote user a message composed of the received nonces N and M, the calculated value T and a HMAC (M, Id_i, S).

d) Upon receiving the message by the remote user, the value S is calculated as follows: (S = N $\oplus$ T) and the message is verified by calculating the associated HMAC. If the check is successful, the remote user also generates a random nonce W on 8 bytes, applies a XOR with value S as: (Z = W $\oplus$ S), and sends to the sensor node a message composed by: the received nonce N, the value Z , the value S, and a HMAC (N, Id_i, W).

e) When the sensor node receives the message, the value W is calculated as follows: (W = Z $\oplus$ S), and the message is verified by calculating the associated HMAC. If the check is successful, mutual authentication between objects terminates successfully.

3) Key establishment phase: Once the authentication phase terminates successfully, a shared symmetric key K is established to secure the communication channel.

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 S and W. Then, the concatenation of the two values K1 and K2, and apply an encryption with the associated secret key of the sensor node X_i. The obtained key K must be on 128 bits.

At the end, an encrypted message *Finished* with the session key K is sent to the remote user to indicate that the key establishment terminates (The message *Finished* contains also the session key K). The remote user, in turn, calculates, decrypts the message, verifies the session key, and stores the shared session key K.

IV. Security analysis of the proposed scheme

In this section, we present a security analysis of the proposed scheme in order to prove its efficiency in the security side. Our proposed authentication scheme provides a resistance to several possible attacks. We are interested especially to:

- *Replay Attack:* Suppose that an attacker intercepts a previous message exchanged in the authentication phase, and tries to replay it in order to impersonate the sensor node respectively the remote user or the gateway node. The attacker cannot successfully impersonate the sensor node, the remote user or the gateway node because new nonces are generated for each authentication to provide mutual authentication.

- *Impersonate a sensor node:* An attacker cannot impersonate a sensor node since his identity is masked by the value $MSId_i$. Also, the attacker cannot impersonate the remote user or the gateway node without calculating a valid HMAC using the sensor identity Id_i.

- *Denial-of-service attack:* The Denial of service (DoS) is an extremely dangerous attack, since the IoT environments are resources constrained. There are different types of DoS attacks, e.g. Jamming, Flooding, Tampering, etc. [15]. We are interested especially to the threat of Flooding attack, which can affect the proposed authentication scheme. A DoS attack is not possible since an exchange in the authentication phase requests a response message. The response indicates the acceptance or rejection of the message, thus knowing that the received message is an authentic one and not a DoS attack. In addition, the proposed authentication scheme is based on random nonces, which are accepted only once in the authentication process. Therefore, it offers resistance against DoS attacks.

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

- *Mutual authentication:* In the authentication phase, both of the authenticity of the sensor node, the gateway node, and the remote user is proven. This process is called mutual authentication. Consequently, both of the sensor node, the gateway node, and the remote user are sure of the authenticity of the received messages.

- *Identity protection:* A masked identity $MSId_i$ is calculated for each sensor node. This value will be also known by the gateway node and the remote user in order to disallow the revelation of the sensor identity Id_i.

- *Data integrity:* In the proposed authentication phase, we make sure that the captured data transmitted between the sensor node, the gateway node, and the remote user, are not altered by using the HMAC verification. This verification is done for each exchanged message.

- *Synchronization independence:* The use of timestamps guarantees the freshness of message, and therefore confirms that is not an old replayed message. This method requires synchronization between objects. Our proposed scheme is resistant against replay attack by the use of random nonces in the different exchanges. Consequently, it enhances the security on the authentication phase, and makes unnecessary the implementation of synchronization.

- *Session key establishment:* At the end of a successful authentication, a shared secret key is established between the sensor node and the remote user. This key is used as a session key to ensure secure communication between the two objects.

- *Scalability:* The scalability concerns the sensor nodes. The scheme is extensible as it allows new sensor nodes to be integrated into the system. A new sensor node is registered into the gateway and the remote user through the registration phase, and therefore added in the security related information table with its masked identity and cipher suite.

As a result of security analysis of the proposed scheme, we conclude that is suitable for an insecure environment in which communications may be eavesdropped by a malicious user. Our authentication scheme uses nonces and HMAC. If the application changes periodically its security key every three months, the probability that the attacker can take advantage of a forged HMAC is extremely low [16].

V. Performance evaluation of the proposed scheme

In order to evaluate the proposed authentication scheme, we focus especially on the energy consumption of the sensor node as a constrained device. We compute the energy required for the execution of the cryptographic primitives along with the energy required for transmitting and receiving data. We use a TelosB sensor node equipped with a CC2420 radio. This

latter typically runs on two AA batteries, which combine about 18500 J.

In our scheme, we use a HMAC [4] in the different authentication exchanges. The HMAC is not calculated by using a block cipher, but by an iterative cryptographic hash function such as MD5 or SHA-1. The hash function divides the message into fixed-size blocks (Our case: 128 bits for MD5) and iterates over them with a compression function. We have used HMAC-MD5 on a selected 4 bytes for our evaluation, which is not affected by the reported collisions in MD5 and SHA-1 [17].

Authors in [18], 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 [16]. The measurement of the electrical energy is calculated using the following function:

$$E = P \times t$$

Where:

E: is the electric energy expressed in joule (J).

P: is the nominal power of the electric dipole expressed in watt (W).

t: is the duration of use expressed in second (s).

Table III summarizes the deduced values, which are used as an energy model for the different operations on the proposed authentication scheme. For the evaluation of the total energy cost, we consider the cost of transmission, reception, and cryptographic operations.

TABLE III. ESTIMATED ENERGY COSTS ON THE SENSOR NODE [16] [18]

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
HMAC-MD5 computation of 32 bytes	62.15 μJ

We evaluate the energy consumption of the proposed authentication scheme in the authentication phase and the key establishment phase. In addition, we study the cases of an authentication failure, and we evaluate the energy consumption in the different cases: F1, F2, F3 and F4 as shown in Table IV.

As described in our scheme, a node has to send its masked identity (20 bytes), the generated nonce value (8 bytes), and calculates the HMAC which requires 62.15 μJ. Thus, the size of the transmitted message is 44 bytes (20 bytes + 8 bytes + 4 bytes of HMAC + 12 bytes of protocol headers) which requires 253.44 μJ to be transmitted. As a response from the remote user, the node receives a 40 bytes message containing three nonces and a HMAC (3*(8 bytes) + 4 bytes of HMAC + 12 bytes of protocol headers) which requires 259.2 μJ to be received, and 62.15 μJ to verify the HMAC. Therefore, the total energy cost of the authentication phase of the proposed scheme is equal to 636.94 μJ.

In the key establishment phase, an encryption of the concatenation of the two values K1 and K2 (result on 16 bytes) requires about 42.88 μJ, and applying the function F if necessary (In our case, the result of the calculation of the shared key K is on 16 bytes, we do not apply the function F). Finally, the encryption of the message *Finished* (16 bytes) with the established shared key K requires 42.88 μJ and 161.28 μJ to be transmitted. Therefore, the total energy cost of the key establishment phase is equal to 247.04 μJ.

The total cost of the full scheme is the cost of the authentication phase plus the cost of the establishment phase: 883.98 μJ. A very low cost proving that our scheme is lightweight and suitable to be applied on WSN applications in a resource constrained IoT environment.

TABLE IV. ANALYSIS OF THE AUTHENTICATION SCHEME

Case of authentication	Energy consumption	Number of sent messages	Number of received messages
F1	315.59 μJ	1	0
F2	315.59 μJ	1	0
F3	315.59 μJ	1	0
F4	636.94 μJ	1	1
Successful authentication	883.98 μJ	2	1

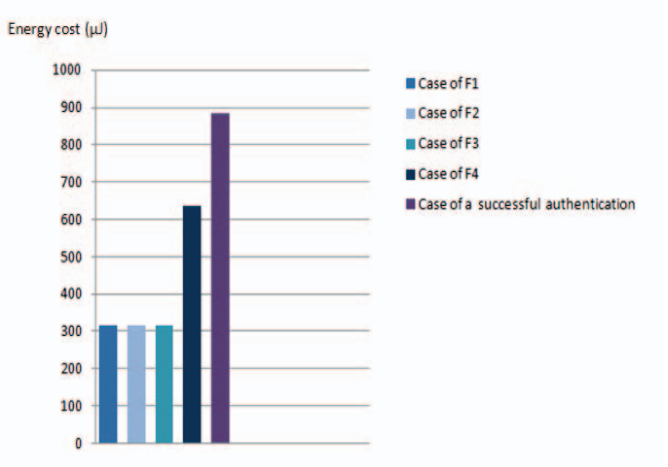

Fig. 4. Energy-cost analysis of the authentication scheme

As a result from this 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 obtained result enhances the scheme performance.

VI. VARIANT OF OUR SCHEME BASED ON A LIGHTWEIGHT PKI

The scheme is also implementable in the case of a pair of key, a public key of the remote user that is only known by the sensor node and the gateway node and a private one that is kept secret for the remote user.

At first, we assume that the public key of the remote user is transmitted to the sensor node in the registration phase. We can truncate the public key on 128 bits, and use it as the secret key X_i in cryptographic functions along with the cipher suite in the authentication phase, or possess another key with the cipher suite. The authentication phase is like the previous proposed authentication phase.

In the next step, we calculate the shared key and then apply the function F if necessary (In our case, the result of the calculation of the shared key K is on 16 bytes, we do not apply the function F). Once the secret shared key is calculated, the encrypted message *Finished* containing the key is sent. The encryption is performed using an ECC [8] that is more energy efficient giving the same level of security as the conventional algorithms such as RSA.

The cost of this variant of the proposed scheme is the same in authentication phase plus 42.88 μJ required for key computation, 17 mJ for the ECC-160 bits encryption [18] of the message *Finished*, and 161.28 μJ for the transmission. Therefore, the total cost is 17.84 mJ.

The result is very interesting compared to energy costs of the authentication scheme proposed in [14], where this latter is applied in the case of authentication with direct access. The energy cost of the proposed authentication scheme is slightly more despite its implementation in the case of a remote user (See figure 5).

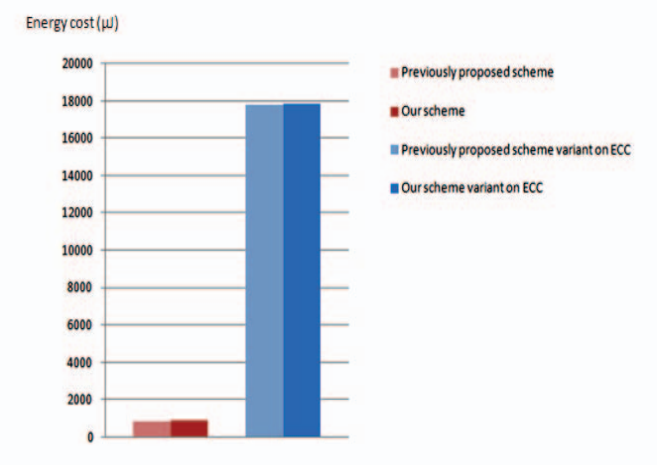

Fig. 5. Energy-cost comparison

VII. Conclusion and future works

In this paper, we have proposed a new lightweight authentication scheme for remote WSN applications in the context of IoT using nonces, masked identity, and HMAC for the different exchanges. The proposed scheme has low costs of communication and computation with a high level of security, and it terminates with a session key establishment. It also saves energy in the different cases of an authentication failure. The scheme is then suitable to be applied in WSN applications deployed in a resource constrained environment. As a future work, we aim to simulate our proposed authentication scheme using Cooja simulator of Contiki OS, and to test it in a real deployment in order to obtain a more accurate analysis study especially on memory consumption and execution time.

References

[1] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 316–323, 2013.

[4] H. Krawczyk, R. Canetti, and M. Bellare, "Hmac: Keyed-hashing for message authentication," 1997.

[5] T. El Maliki and J.-M. Seigneur, "A survey of user-centric identity management technologies," in *Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007. The International Conference on*. IEEE, 2007, pp. 12–17.

[6] E. Rescorla and N. Modadugu, "Datagram transport layer security version 1.2," 2012.

[7] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "Dtls based security and two-way authentication for the internet of things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2710–2723, 2013.

[8] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "Nanoecc: Testing the limits of elliptic curve cryptography in sensor networks," in *Wireless sensor networks*. Springer, 2008, pp. 305–320.

[9] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed iot applications," in *Wireless Communications and Networking Conference (WCNC), 2014 IEEE*. IEEE, 2014, pp. 2728–2733.

[10] ——, "Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014.

[11] *SEC4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV), version 0.97*. www.secg.org, August 2013.

[12] M. Turkanović, B. Brumen, and M. Hölbl, "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*, vol. 20, pp. 96–112, 2014.

[13] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment," *Ad Hoc Networks*, vol. 36, pp. 152–176, 2016.

[14] H. Khemissa and D. Tandjaoui, "A lightweight authentication scheme for e-health applications in the context of internet of things," in *Next Generation Mobile Apps, Services and Technologies (NGMAST), 2015 Ninth International Conference on*. IEEE, 2015, pp. 90–95.

[15] A. D. Wood, J. Stankovic *et al.*, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[16] J. Lee, K. Kapitanova, and S. H. Son, "The price of security in wireless sensor networks," *Computer Networks*, vol. 54, no. 17, pp. 2967–2978, 2010.

[17] B. Schneier, "Schneier on security: Sha-1 broken," *URL: http://www.schneier.com/blog/archives/2005/02/sha1_broken.html, (February 2005) [Last Accessed: May 2015]*, 2005.

[18] G. De Meulenaer, F. Gosset, O.-X. Standaert, and O. Pereira, "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,*. IEEE, 2008, pp. 580–585.