D. Galindo, R. Roman, and J. Lopez, "A Killer Application for Pairings: Authenticated Key Establishment in Underwater Wireless Sensor Networks", *Proceedings of the 7th International Conference on Cryptology and Network Security (CANS08)*, LNCS vol. 5339, pp. 120-132, 2008.
http://doi.org/10.1007/978-3-540-89641-8_9
NICS Lab. Publications: https://www.nics.uma.es/publications

A Killer Application for Pairings: Authenticated Key Establishment in Underwater Wireless Sensor Networks

David Galindo[1]*, Rodrigo Roman[2] and Javier Lopez[2]

[1] University of Luxembourg
david.galindo@uni.lu
[2] Department of Computer Science, University of Malaga, Spain
{roman,jlm}@lcc.uma.es

Abstract. Wireless sensors are low power devices which are highly constrained in terms of computational capabilities, memory, and communication bandwidth. While battery life is their main limitation, they require considerable energy to communicate data. The latter is specially dramatic in underwater wireless sensor networks (UWSN), where the acoustic transmission mechanisms are less reliable and more energy-demanding. Saving in communication is thus the primary concern in underwater wireless sensors. With this constraint in mind, we argue that non-interactive identity-based key agreement built on pairings provides the best solution for key distribution in large UWSN when compared to the state of the art. At first glance this claim is surprising, since pairing computation is very demanding. Still, pairing-based non-interactive key establishment requires minimal communication and at the same time enjoys excellent properties when used for key distribution.

Keywords: identity-based key agreement, underwater wireless sensor networks, key distribution, pairings.

1 Introduction

Sensors are inexpensive, battery-powered devices which have limited resources. A wireless sensor node typically consists of a power unit, a sensing unit, a processing unit, a storage unit and a wireless transmitter and receiver. Security is one of the principal concerns while designing protocols and mechanisms for wireless sensor networks (WSN). They usually are not tamper-resistant due to cost constraints, and it is easy to physically access them in most scenarios because they must be located near the physical source of the events. Furthermore, any device can access the information exchange because the communication channel is public.

* Work done while the author was with the University of Malaga.

It is easy the for an adversary to manipulate the sensor nodes and the communication channel of an unprotected network on its own benefit.

Security protocols require the existence of some security credentials (i.e. pairwise keys) between peers in order to encrypt, authenticate and provide integrity to the information flow. Key distribution is not trivial in WSN because in most cases it is not possible to know in advance which nodes are going to be neighbors, that is, which nodes need to share a pairwise key.

It is well-known that from an efficiency point of view, symmetric key cryptography outperforms public (or asymmetric) key cryptography. Indeed, public key primitives are of the order of hundred of times more computationally intensive that their symmetric key counterparts. The development of an efficient key management system (KMS) for creating pairwise keys between neighbors is a hot research topic, with many complex symmetric key cryptography based frameworks [AR06]. The better performance of symmetric key primitives can be even more acute in resource-constrained devices, for which frequently battery life is the main limitation, so the less computationally expensive (and hence less energy consuming) operations the better. This is the reason why in areas like wireless sensor network security, using public key cryptography has been considered prohibitive from the very beginning.

Somewhat surprisingly, this common wisdom is being challenged. The main reason behind this is the fact that communicating data in these devices requires considerable power, in contrast to wired devices. Therefore, it can be the case that the energy saving of a computationally inexpensive primitive is nullified by the bigger amount of data it requires to be sent. This has already been shown by Großschädl, Szekely and Tillich in [GST07], where the energy cost of two standardized symmetric and asymmetric key exchange protocols has been evaluated. Specifically, the symmetric key protocol used in that study is a light-weight variant of authenticated Kerberos [KN93], while the asymmetric key protocol is an elliptic curve version of Menezes-Qu-Vanstone [MQV95,DE06] (ECMQV). The striking result is that in standard medium-size wireless sensor networks, ECMQV consumes less power than Kerberos, due to the fact that it requires 50% less bits to be exchanged.

We go one step further by considering an extreme case of wireless communication, namely, communication between underwater sensor nodes. Classical electromagnetic waves communication is not satisfactory in underwater environments due to the conducting nature of the medium, especially in the case of sea water. Instead, acoustic communication is the most widely used technique, due to the low signal reduction of sound in water [LZC08]. Acoustic communication presents severe limitations in bandwidth and requires a huge amount of energy. According to Morgansen [Hic08], current state of the art in practical scenarios is transmission of 640 bits (80 bytes) per second. We argue than in this extremely constrained environment, non-interactive identity-based key establishment (NIKE) protocols such as SOK [SOK01,DE06] provides the most efficient solution to the problem of key distribution in large UWSN. This can seem quite surprising, since at the time of this writing efficient identity-based key cryptography is tied to a computational number-theoretic primitive called bilinear pairing (cf. Chapter 5 in [BSS05]), which is a computationally intensive operation. In a wired system, identity-based key agreement would in general only be used for its specific functionalities, but not from a computational efficiency point of view. At first sight, one would preclude its use in WSN for a similar reason. However, the use of NIKE in UWSN achieves the lowest bandwidth while providing the best properties for key distribution from a global point of view.

The structure of this paper is as follows: In Section 2 we revise the concept of wireless sensor networks and the need of key management systems with certain properties. Later, in the same section, we introduce the special features of underwater sensor networks (UWSN). In Section 3, we will revise the behaviour of non-interactive identity-based key agreement protocols, and analyze their suitability to UWSN in comparison with other “traditional” asymmetric protocols. In Section 4, we evaluate whether symmetric key-based KMS are more useful in underwater environments than identity-based protocols. Finally, in Section 5 we conclude the paper.

2 Wireless Sensor Networks

Wireless sensor networks are a very useful tool for solving problems in scenarios that require the acquisition and processing of physical measurements. The principal elements of a sensor network are the sensor nodes and the base station. Sensor nodes (nodes) are wireless-enabled, battery-powered, highly constrained devices that collect the physical information from their environment using an array of sensors such as thermistors, photodiodes, and so on. The base station is a more powerful device that serves as an interface between the nodes and the user. It collects the information coming from sensor nodes, and also send control information issued by the user. There can be from dozens to thousands of sensor nodes on a deployment field, although there is usually only one or more base stations on the same field.

Security is one of the principal concerns while designing protocols and mechanisms for WSN. In fact, sensor networks are inherently insecure due to the features of their nodes and the communication channel. As a result, it is easy for an adversary to manipulate the sensor nodes and the communication channel of an unprotected network on its own benefit. There must be some protocols and security mechanisms that guarantee the resiliency of the network against any kind of external or internal threat. The foundation of these mechanisms and protocols are the security primitives, such as Symmetric Key Cryptography (SKC), Public Key Cryptography (PKC) and Hash functions. Using these primitives, it is possible to assure the confidentiality and integrity of the communication channel, while authenticating the peers involved in the information exchange.

Due to its energy efficiency and fast speed, Symmetric Cryptography becomes an interesting choice for securing the foundations of a sensor network. It can provide confidentiality to the information flow, and is also able to provide integrity. There are many optimal SKC algorithms implemented on sensor networks (such as Skipjack), that have small requirements in terms of memory usage and encryption speed (2600 bytes and 25μs/byte for Skipjack, respectively [CS06]). Moreover, some sensor nodes have transceivers that implement the IEEE 802.15.4 standard, which include a hardware implementation of the AES-128 algorithm.

However, as aforementioned, it is necessary to have certain security credentials in order to open a secure channel between two peers. As a result, if a sensor network relies only on SKC, it is necessary to implement certain key management systems (KMS) that distribute the pairwise keys over the nodes of the network before or after its deployment. The underlying problem here is the typical key management shortcomings of symmetric-key algorithms. To have a glance at these shortcomings, let us introduce some metrics to evaluate key distribution solutions, in particular, those proposed in [CY05,AR06]:

- **Scalability**: Ability to support large networks.
- **Efficiency**: Storage, processing and communication limitations on sensor nodes must be considered:
  - **Storage**: Amount of memory required to store security credentials.
  - **Processing**: Amount of processor cycles required to establish a key.

  - **Communication**: Number of messages exchanged during a key generation process.
  - **Key connectivity**: Probability that two (or more) sensor nodes store the same key or keying material.
- **Resilience**: Resistance against node capture.
- **Extensibility**: Key distribution mechanisms must be also flexible against substantial increase in the size of the network after deployment.

Typical shortcomings of SKC-based key distribution solutions are associated to either scalability, key connectivity, resilience and extensibility properties, being the main advantage of these solutions a low processing time. Public Key Cryptography (PKC) is useful in this context. By using authenticated key exchange protocols, the process of negotiating pairwise keys between previously unknown peers can be greatly simplified, as it enjoys benefits in every single property in the above-mentioned metrics, except for processing time. However, as we shall see, in UWSN the processing time gets its relevance lowered, as bandwidth is by far the most relevant parameter. Thanks to this, a specialized PKC-based key establishment mechanism, namely, non-interactive identity-based key agreement, outperforms previous SKC-based key distribution solutions.

2.1 Underwater Wireless Sensor Networks

The cost of using the communication channel largely impacts the energy required to run any interactive protocol between sensor nodes. Most previous analysis were done considering a sensor node that uses the air as a transmission medium. This is the most common situation for a WSN, and most prototypes have been deployed on such conditions. However, there are many potential applications where sensor nodes must be deployed in a lake or in the sea, either for long-term aquatic monitoring (Marine biology, deep-sea archaeology, seismic predictions, pollution detection, oil/gas field monitoring) or short-term aquatic exploration (Underwater natural resource discovery, anti-submarine mission, loss treasure discovery) [Cui07]. These networks have received the generic name of Underwater Sensor Networks (UWSN) [APM05].

In these UWSN, it is unpractical to use radio frequency transceivers, because of the severe attenuation factor presented by water. In order to open a communication channel between sensors, it is necessary to use specific underwater acoustic modems. These modems have different features than RF transceivers: they are highly unreliable, their bandwidth is much more limited, and sending or receiving one bit of information carries a high energy penalty.

The differences between radio transceivers and acoustic modems in terms of the energy consumed by transmitting and receiving one single bit of data are highlighted in Table 1. It can be seen that the difference in consumption (J per bit) between acoustic modems and RF transceivers is not negligible. For the radio transceivers, we have considered the most popular sensor nodes platforms as of today, which are the MICA2 and the MICAz [Inc08]. The MICA2 transceivers use the 868/916 MHz ISM bands, while the MICAz transceivers use the IEEE 802.15.4 standard. For the acoustic modems, we have considered the UWM2000 and UWM4000 modems [Inc07], which are commonly used in research literature.

These results have been obtained using the information contained in the modem and mote datasheets, under the following assumptions: i) For the UWM2000 modem, we have used the mean of the transmission power indicated in its datasheet (2-8W). ii) For the transceivers used in the MICA2 and MICAz motes, we have considered the most expensive transmission mode, which is theoretically able to send a bit of data to the maximum working range.

	MICA2	MICAz	UWM2000	UWM4000
Working range	150 m	100 m	1500 m	4000 m
Throughput	19.2 kbit/s	250 kbit/s	9600 bit/s	4800 bit/s
Tx. consumption	81mW	52.2mW	4000 mW	7000 mW
Rx. consumption	30mW	59.1mW	800 mW	800 mW
μJ per bit (Tx)	4.12 μJ	0.204 μJ	416.66 μJ	1458.33 μJ
μJ per bit (Rx)	16.8 μJ	16.8 μJ	83.33 μJ	166.66 μJ

Table 1. Analysis of the energy consumption of acoustic modems.

3 Non-interactive identity-based key agreement

If one uses traditional PKC-based authenticated key agreement to build key distribution solutions, then one is forced to use certificates, since they are needed to establish a trusted link between a public key and the identity of its owner (in our case a sensor node) in order to prevent man-in-the-middle attacks. In a WSN, nodes are supposed to establish pairwise keys with nodes that belong to the same network, and forbidden to do so with nodes or devices outside the network. Therefore, in key establishment protocols like ECMQV, the nodes must at the beginning exchange their public keys and certificates. It is natural to assume these certificates take the form of a signature by the base station on the identity and public key of the node. In general, nodes public and secret keys are set up by the base station. Such a setting can be viewed as a key-escrowed system, that is, there exists a trusted party who computes the secret keys of the users. As a consequence, one is tempted to use different forms of key-escrowed public key paradigms like identity-based cryptography, even if they do not provide certain properties such as forward secrecy.

The concept of identity-based cryptography was proposed by Shamir in [Sha85], aimed at simplifying certificate management inherent to the deployment of public key cryptography. The idea is that an arbitrary string id uniquely identifying a user (such as an e-mail address or a telephone number) can serve as a public key for a cryptographic scheme. The user cannot compute the corresponding secret key anymore, but instead it must authenticate itself to a Key Generation Center from which it obtains the corresponding private key $sk[id]$ via a secret channel.

The interest of IBC for WSN is that when using IBC systems only the identity of the sensors must be exchanged, and thus neither public keys nor certificates need not be sent. This results in an energy saving for the point of view of the communication between sensors, which can be very considerable depending on the sensor's transmitter. Additionally, in WSN it is often the case that a single party (base station) sets up the network, and this base station can naturally play the role of the Key Generation Center in an IBC system. The base station embeds the secret key $sk[id]$ prior its use in the field, and no authentic nor secret channel is needed for key setup.

In this section we recall a non-interactive authenticated identity-based key establishment scheme. Due to the lack of any standardized identity-based key exchange protocol, we describe a non-interactive scheme due to Sakai, Ohgishi and Kasahara [SOK01,DE06], which is the first identity-based authenticated key agreement protocol proposed in the literature. Also, for comparison purposes, the elliptic curve version of the Menezes-Qu-Vanstone authenticated key exchange protocol [MQV95,LMQ$^+$03], which is one of the most standardized key exchange protocol using public key cryptography, is described in Algorithm 3.2. Note that we provide an abridged version of both schemes which suffices for our purposes. Moreover, we consider that the involved nodes must exchange their credentials due to extensibility issues (preexisting nodes may not have the public credentials of new nodes) and memory issues (nodes may not be able to store the credentials of all the nodes of the network).

3.1 SOK - Sakai, Ohgishi and Kasahara

We start by defining the concept of bilinear map. Let $\mathbb{G} = \langle \mathbf{g} \rangle$ be a cyclic group of order q for prime $q > 3$. A map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ to a group $\mathbb{G}_1$ is called a *bilinear* map, if it satisfies the following two properties:

Bilinearity: $e(\mathbf{g}^a, \mathbf{g}^b) = e(\mathbf{g}, \mathbf{g})^{ab}$ for all integers a, b
Distorted: $e(\mathbf{g}, \mathbf{g}) \neq 1$ in $\mathbb{G}_1$.

See [BF03,Ver04] for ways of constructing bilinear maps.

In the SOK protocol, a hash function $H : \{0,1\}^* \to \mathbb{G}$ is included in the domain parameters of the system, together with $\mathbf{g}^z$, where the master secret key z is only known to the base station. Node A's secret key is $sk_A = H(id_A)^z$, while node B's secret key is defined as $sk_B = H(id_B)^z$. Notice that A's identity is id_A and B's identity is id_B.

Algorithm 3.1 SOK non-interactive ID-based key derivation for entity A

```
Input: Bilinear map domain parameters $\mathbb{G}, \mathbb{G}_1, e, \mathbf{g}^z, n$, the identity $id_B$
    and the secret key $sk_A$
Output: A secret key $K_{AB}$ shared with entity with identity $id_B$
$K_{AB} \leftarrow KDF(e(H(id_B), sk_A))$
```

Entity B runs the same algorithm by simply swapping the values (id_B, sk_A) in Algorithm 3.1 with (id_A, sk_B) and finally obtains the same key K_{AB} thanks to the bilinearity of the pairing,

$$\begin{aligned} e(H(id_B), sk_A) &= e(H(id_B), H(id_A)^z) = e(H(id_B), H(id_A))^z = \\ &= e(H(id_A)^z, H(id_B)) = e(sk_B, H(id_A)) \end{aligned}$$

3.2 ECMQV - Elliptic Curve Menezes-Qu-Vanstone

In the following we define the notation and behaviour of ECMQV. KDF is a key derivation function, which can be implemented with SHA-160 for example. Node A's public key is $\mathrm{pk}_A = g^{x_A}$, where x_A is A's secret key. Similarly for node B. In the first stage, the nodes exchange and verify certificates vouching for the fact that pk_A and pk_B are public keys from nodes belonging to the network. In a second stage, they exchange their ephemeral keys $E_A = g^{y_A}$ and $E_B = g^{y_B}$, where y_A, y_B are taken at random from the finite field GF(p). We assume certificates are minimalist and take the form of ECDSA [X905] signatures (r_A, s_A) and (r_B, s_B) by the owner/manufacturer of the network on the messages $id_A||\mathrm{pk}_A$ and $id_B||\mathrm{pk}_B$ respectively, where || denotes concatenation.

Algorithm 3.2 ECMQV key derivation for entity A

```
Input: Elliptic curve domain parameters $G, g, n$, the secret keys $x_A, y_A$
    and the public elements $\mathrm{pk}_A, \mathrm{pk}_B, E_A, E_B$
Output: A secret key $K_{AB}$ shared with entity with public key $\mathrm{pk}_B$
$m \leftarrow \lceil \log_2(n) \rceil / 2$    $\{m$ is the half bitlength of $n\}$
$u_A \leftarrow (u_x \bmod 2^m) + 2^m$    $\{u_x$ is the $x$-coordinate of $E_A\}$
$s_A \leftarrow (y_A + u_A x_A) \bmod n$
$v_A \leftarrow (v_x \bmod 2^m) + 2^m$    $\{v_x$ is the $x$-coordinate of $E_B\}$
$z_A \leftarrow s_A v_A \bmod n$
$K_{AB} \leftarrow KDF(E_B^{s_A} \cdot \mathrm{pk}_B^{z_A} \bmod n)$
```

Entity B runs the same algorithm by simply swapping the values $(x_A, y_A, \mathrm{pk}_B, E_A, E_B)$ in Algorithm 3.2 with $(x_B, y_B, \mathrm{pk}_A, E_A, E_B)$ and finally obtains the same key K_{AB} (cf. [LMQ+03]).

3.3 Bandwidth and energy consumption

As we can see, the SOK protocol only requires the identities id_A, id_B of the sensors involved to compute a pairwise authenticated and confidential key. On the other hand, the communication overhead of the ECMQV protocol is dominated on by the exchange of public keys, certificates and ephemeral keys. On the computational side, SOK has to perform one hash operation, which is roughly equivalent to 1 exponentiation in $\mathbb{G}$ '$\exp_{\mathbb{G}}$', plus 1 pairing computation. ECMQV has to verify an ECDSA signature (one multi-exponentiation 'mexp(2)'), and to run its protocol (one multi-exponentiation 'mexp(2)', one exponentiation 'exp', and two square roots 'sqrt' to obtain the y-coordinate from the x-coordinate). Consequently, the overall energy cost and transmission cost of ECMQV for one node amounts to:

$$2\mathrm{mexp}(2) + 1\mathrm{exp} + 2\mathrm{sqrt}(+\mathrm{trans.}\ 1410\ \mathrm{bits} + \mathrm{recep.}\ 1410\ \mathrm{bits}) \qquad (1)$$

whereas the energy cost and transmission cost of SOK for one node amounts to:

$$1\exp_{\mathbb{G}} + 1\text{pairing}(+\text{trans. } 384 \text{ bits} + \text{recep. } 384 \text{ bits}) \qquad (2)$$

considering that i) one packet containing nodes identities, protocol ID, message ID, checksum, and low-level headers and footers, amounts to a total of 384 bits, ii) public keys have 161 bits (160 bits + 1 compression bit), iii) each ECDSA certificate has 320 bits, and iv) each ephemeral key contributes with 161 bits.

The SOK protocol only needs to exchange 384 bits, whereas the ECMQV protocol must exchange 1410 bits. Therefore, the SOK protocol requires the lowest bandwidth to accomplish its task. In fact, due to the unreliable nature of the acoustic channel, it is much better to use a protocol that exchanges as few bits as possible. The main limitation of the SOK protocol is the pairing computation, as it is very energy consuming. The most efficient implementation we are aware of is to be found in [OSLD08], where it is reported that a pairing for an 80-bit security level (RSA-1024 equivalent) in the ATmega128L microcontroller [Cor07] (one of the most popular microcontrollers for sensor nodes, featuring a 8-bit/7.3828 processor, 128 KB flash memory and 4KB SRAM memory) takes about 5.45s processing time and has around 125mJ energy cost. This is a rather large figure, but if we compare this amount of energy to that needed to transmit data in the UWM2000 and UWM4000 underwater sensors, we obtain that computing a pairing takes the same amount of energy than transmitting 300 and 85 bits respectively! Thus, put into perspective, computing a pairing in UWSN cannot be considered prohibitive at all.

MICA2	Comp.	Comm.		**MICAz**	Comp.	Comm.	
ECMQV	107.26	7.95	*115.21*	ECMQV	107.26	0.61	*107.87*
SOK	309.39	2.16	311.55	SOK	309.39	0.166	309.55

UWM2000	Comp.	Comm.		**UWM4000**	Comp.	Comm.	
ECMQV	107.26	704.98	812.24	ECMQV	107.26	2291.23	2398.49
SOK	309.39	191.99	*501.38*	SOK	309.39	623.99	*933.38*

Table 2. Energy cost of authenticated key exchange (in mJ)

This assertion is backed up by the results shown in table 2, which uses the energy figures for elliptic curve computations and pairing computations of [SOS+08] to calculate the energy consumption of a sensor node engaged in authenticated key exchange protocols in “normal” and underwater sensor networks, in terms of mJ. The results are not surprising, since the cost of sending one bit through an acoustic channel is much greater than sending one bit through a radio frequency channel, and the transmission cost on SOK is much smaller than the transmission cost of ECMQV.

4 NIKE and Symmetric Key-based KMS

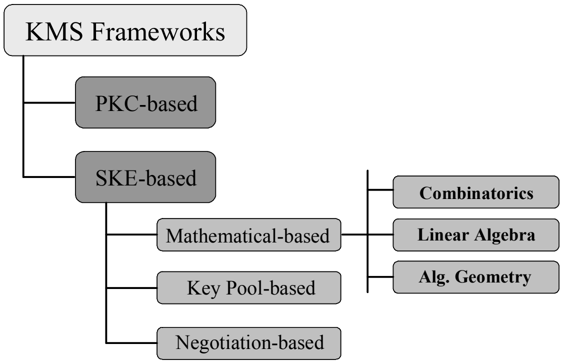

Fig. 1. KMS frameworks for WSN

Although we have shown that non-interactive identity-based key agreement (NIKE) protocols like SOK are better than traditional asymmetric key establishment protocols (e.g. ECMQV) in underwater environments, it is also important to compare them with symmetric key-based KMS. The problem of creating a secure and efficient key management system for sensor networks based on Symmetric Cryptography has spanned three major frameworks: “Key-Pool” framework, Mathematical framework and Negotiation framework (see Figure 1). In the “Key-Pool” framework, every node stores a small subset of keys (known as “key chain”) retrieved from a large set of precalculated key (known as “key pool”). Two nodes will share a pairwise key if they have a common key inside their “key chains”. In the Mathematical framework, two nodes calculate a common pairwise key using mathematical concepts belonging to the fields of Linear Algebra, Combinatorics and Algebraic Geometry. Lastly, in the Negotiation framework, sensor nodes exchange information related to their pairwise keys just after the deployment of the network.

Most KMS belonging to any of the three major frameworks must exchange certain information (e.g. the indexes of the keys included inside a "key chain") in order to derive a pairwise key. Therefore, in terms of bandwidth and energy usage, they are not better than NIKE protocols for underwater environments. However, inside every framework there are some KMS that are optimized to minimize the communication overhead, even reducing the amount of information exchanged to only the ID of a node. Some "key pool" KMS reduce the communication overhead by linking the contents of the "key chains" to the IDs of the nodes [MHH05]. Also, in certain mathematical frameworks, the IDs of the nodes will be used as an input for a function that will return the pairwise key: Polynomial-based key predistribution KMS calculate $f(ID_i, ID_j) = f(ID_j, ID_i)$ (being f a bivariate polynomial) [LNL05], whereas Blom-based key predistribution KMS calculate $A(ID_i) \cdot G(ID_j) = A(ID_j) \cdot G(ID_i)$ (being A and G specially crafted matrices)) [DDH$^+$05]. Finally, some negotiation KMS only need to broadcast small nonces that can be further combined into pairwise keys [LHKV04].

While all these optimized protocols could be used for underwater environments due to their low communication overhead, they have certain disadvantages that discourage their use in this particular environment. In "key pool"-related KMS, both their connectivity and their resilience is not good. As a result, there exists the possibility of two nodes not sharing a pairwise key, thus it is necessary to start expensive negotiations through the acoustic channel. Besides, if an adversary captures enough nodes of the network, it will obtain information of the pairwise keys shared by other nodes. The resilience of mathematical-based KMS is also deficient. This is not the only disadvantage of this framework: the scalability and the extensibility of the Blom scheme is unsatisfactory, and the security of both mathematical foundations (Blom schemes and bivariate polynomials) has not been formally demonstrated. About negotiation-based KMS, the security of the exchange of pairwise keys can usually be assured only just after the deployment of the network. Therefore, an adversary can eavesdrop the negotiation process of either new nodes that want to establish communication with old nodes or nodes that move from their original position and want to open a secure channel with their new neighbourhood.

In comparison with all these optimized symmetric key-based KMS, non-interactive identity-based key agreement protocols like SOK offers better scalability, key connectivity, extensibility, and network resilience. The amount of information that has to be stored inside the nodes is independent of the size of the network, thus there are no size restrictions. Also, all nodes can exchange their IDs at any given time, thus it is possible to open a secure connection between any pair of nodes and to add new nodes to the network. Moreover, if an adversary captures a sensor node, it will only obtain the information related to the node, thus he/she will be unable to eavesdrop any ongoing communication between other nodes. The primary downside of non-interactive identity-based key agreement is its energy consumption. However, the enhanced properties of this pairing-based key agreement (e.g. better extensibility) makes it a good candidate for real-life situations and scenarios. Besides, due to special requirements such as node mobility [Hic08], the batteries of underwater sensor nodes should have a higher capacity. As a result, the execution of few pairings during the lifetime of the network will not have a great influence in the node.

5 Conclusions

In this work we have focused on the fact that underwater wireless sensor networks consume a huge amount of energy in sending and receiving data. We have studied how identity-based cryptography can help to improve the energy cost of cryptographic key agreement between peers in UWSN. If previous work in the context of standard wireless sensor networks brought the novelty that the energy penalty of transmitting data made an asymmetric key agreement protocol energy-wise more efficient than a symmetric key protocol like Kerberos, our results bring the news that a computationally intensive primitive like non-interactive identity-based key agreement *outperforms* existing key distribution solutions in underwater wireless sensor networks. Future work includes implementing and evaluating identity-based key agreement in real underwater sensor nodes.

Acknowledgements

The authors wish to thank Prof. Gene Tsudik and Dr. Roberto Di Pietro for their useful input during the development of this paper.

This work has been partially supported by the ARES CONSOLIDER project (CSD2007-00004) and the CRISIS project (TIN2006-09242). The second author was funded by the Ministry of Education and Science of Spain under the “Programa Nacional de Formacion de Profesorado Universitario”.

References

[APM05] I. Akyildiz, D. Pompili and T. Melodia. Underwater acoustic sensor networks: Research challenges. *Ad Hoc Networks Jounal (Elsevier)*, 3(3):257–279, 2005.

[AR06] Cristina Alcaraz and Rodrigo Roman. Applying key infrastructures for sensor networks in cip/ciip scenarios. In *1st International Workshop on Critical Information Infrastructures Security (CRITIS 2006)*, pp. 166–178, 2006.

[BF03] D. Boneh and M. Franklin. Identity-Based encryption from the Weil pairing. *SIAM Journal of Computing*, 32(3):586–615, 2003. This is the full version of an extended abstract of the same title presented at *Crypto'01*.

[BSS05] I.F. Blake, G. Seroussi and N. Smart. *Advances in Elliptic Curve Cryptography*, vol. 317 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 2005.

[Cor07] Atmel Corporation. Atmega128 product description. `http://www.atmel.com/dyn/products/product_card.asp?part_id=2018`, 2007.

[CS06] K. Jun Choi and J.-I. Song. Investigation of feasible cryptographic algorithms for wireless sensor network. In *Proceedings of the 8th International Conference on Advanced Communication Technology (ICACT 2006)*, 2006.

[Cui07] Jun-Hong Cui. Underwatersensor network lab — overview, achievements, plans. `http://uwsn.engr.uconn.edu`, 2007.

[CY05] S. A. Camtepe and B. Yener. Key distribution mechanisms for wireless sensor networks: a survey. Technical Report TR-05-07, College of William & Mary, March 2005.

[DDH$^+$05] W. Du, J. Deng, Y. S. Han, P. Varshney, J. Katz and A. Khalili. A pairwise key pre-distribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security*, 8(2):228–258, 2005.

[DE06] Régis Dupont and Andreas Enge. Provably secure non-interactive key distribution based on pairings. *Discrete Applied Mathematics*, 154(2):270–276, 2006.

[GST07] Johann Großschädl, Alexander Szekely and Stefan Tillich. The energy cost of cryptographic key establishment in wireless sensor networks. In *ASIACCS*, pp. 380–382. ACM, 2007.

[Hic08] H. Hickey. Underwater communication: Robofish are the ultimate in ocean robots, keeping in touch without scientists' help, June 2008.

[Inc07] LinkQuest Inc. Underwater acoustic modems. `http://www.link-quest.com/`, 2007.

[Inc08] Crossbow Technology Inc. Wireless sensor nodes. `http://www.xbow.com/`, 2008.

[KN93] John T. Kohl and B. Clifford Neuman. The Kerberos network authentication service (V5), 1993.

[LHKV04] B. Charles Lai, D.D. Hwang, S. Pete Kim and I. Verbauwhede. Reducing radio energy consumption of key management protocols for wireless sensor networks. In *Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED 2004)*, pp. 351–356, 2004.

[LMQ$^+$03] Laurie Law, Alfred Menezes, Minghua Qu, Jerry Solinas and Scott A. Vanstone. An efficient protocol for authenticated key agreement. *Des. Codes Cryptography*, 28(2):119–134, 2003.

[LNL05] D. Liu, P. Ning and R. Li. Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and System Security*, 8(1):41–77, 2005.

[LZC08] Lanbo Liu, Shengli Zhou, and Jun-Hong Cui. Prospects and problems of wireless communications for underwater sensor networks. *Wireless Communications and Mobile Computing - Special Issue on Underwater Sensor Networks,*, 2008. To appear.

[MHH05] M. Mehta, D. Huang and L. Harn. Rink-rkp: A scheme for key predistribution and shared-key discovery in sensor networks. In *Proceedings of the 24th IEEE International Performance Computing and Communications Conference (IPCCC'05)*, pp. 193–197, 2005.

[MQV95] Alfred Menezes, Minghua Qu and Scott Vanstone. Some new key agreement protocols providing mutual implicit authentication. SecondWorkshop on Selected Areas in Cryptography (SAC 95), 1995.

[OSLD08] Leonardo B. Oliveira, Michael Scott, Julio Lopez and Ricardo Dahab. Tinypbc: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. In *5th International Conference on Networked Sensing Systems*, 2008. *To appear.* Available at `http://eprint.iacr.org/2007/482`.

[Sha85] A. Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO 1984*, vol. 196 of *LNCS*, pp. 47–53, 1985.

[SOK01] R. Sakai, K. Ohgishi and M. Kasahara. Cryptosystems based on pairing over elliptic curve (in japanese). In *The 2001 Symposium on Cryptography and Information Security*, 2001. Oiso, Japan.

[SOS$^+$08] P. Szczechowiak, L.B. Oliveira, M. Scott, M. Collier and R. Dahab. Nanoecc: Testing the limits of elliptic curve cryptography in sensor networks. In *Proceedings of the European conference on Wireless Sensor Networks (EWSN'08)*, pp. 305–320, 2008.

[Ver04] Eric R. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *J. Cryptology*, 17(4):277–296, 2004.

[X905] Accredited Standards Committee X9. American national standard x9.62-2005, public key cryptography for the financial services industry, the elliptic curve digital signature algorithm (ecdsa), 2005.