Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Constant round group key agreement protocols: A comparative study

*Eleftheria Makri, Elisavet Konstantinou**

Laboratory of Information and Communication Systems Security, Department of Information and Communication Systems Engineering, University of the Aegean, Karlovassi, GR-82300 Samos, Greece

ARTICLE INFO

Article history:
Received 12 April 2011
Received in revised form
19 August 2011
Accepted 26 August 2011

Keywords:
Constant round
Group key agreement protocols
Communication cost
Computation cost
Energy consumption
Survey
Cryptography

ABSTRACT

The scope of this paper is to review and evaluate all constant round Group Key Agreement (GKA) protocols proposed so far in the literature. We have gathered all GKA protocols that require 1,2,3,4 and 5 rounds and examined their efficiency. In particular, we calculated each protocol's computation and communication complexity and using proper assessments we compared their total energy cost. The evaluation of all protocols, interesting on its own, can also serve as a reference point for future works and contribute to the establishment of new, more efficient constant round protocols.

1. Introduction

During the last decades, collaborative applications (such as multimedia conferencing, distributed simulations, multi-user games and replicated servers) have become extremely popular. All these applications are executed through Internet connections that in most cases should be properly secured. In addition, wireless networks, mobile ad hoc networks and sensor networks are used extensively in many areas of interest (ranging from homes, schools and universities to inaccessible terrains, disaster places, etc.), where security is really crucial.

The realization of such efficient, robust and secure environments is a challenging algorithmic and technological task. All users that participate in the particular application should be able to communicate securely and exchange information that is inaccessible to any external entity. Hence, there is a need for finding new protocols that provide such confidential communication, termed usually as Secure Group Communication or Secure Conferencing. The goal of such protocols is to establish a common secret key among the users, called group key, which can be used for data encryption between them.

A group key management protocol is responsible for the establishment and maintenance of a group key. This secret group key must be distributed in a secure and efficient way to all members of the group. Group key establishment protocols can be divided into two subcategories: the Key Transfer Protocols and the Key Agreement Protocols. During the execution of a Key Transfer Protocol an entity creates or obtains a secret value, which transmits it securely to the rest of the entities. In a Group Key Agreement (GKA) Protocol,

* Corresponding author.
E-mail addresses: eleftheria.makris@gmail.com (E. Makri), ekonstantinou@aegean.gr (E. Konstantinou).

0167-4048/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2011.08.008

a shared secret is derived as a function of information contributed by or associated with all the members in the group, such that no party in the group can predetermine the resulting value.

Clearly, group key establishment and in particular, group key agreement is a fundamental cryptographic primitive. The implementation of such protocols allows a group of parties to agree upon a common session key, which allows them to communicate confidentially through an insecure network. In many cases, the communication cost required for the establishment of the secret group key is of high importance. There are network environments, where the number of communication rounds of a GKA protocol plays a crucial role. Obviously, it is really important in many applications that the number of rounds is constant and thus not affected by the number of users. In many cases the number of rounds is a logarithmic or linear function of the number of group members and thus, as the group increases so does the number of rounds.

1.1. *Our contribution*

The goal of this work is to provide a complete survey concerning all the Constant Round Group Key Agreement Protocols proposed so far in the literature. We have grouped the seventy-nine (79) different protocols into four categories, according to the number of required rounds in each protocol. These four categories were also divided in several subclasses based on some basic features of the protocols, such as authentication, the use of hash functions, the presence of a third party etc.

Beside the presentation of all proposed protocols concerning this field, we also provide a comparative performance evaluation of the examined protocols. Our performance evaluation concerns the computation cost of the protocols in question, their communication cost, as well as their total energy cost. The performance evaluation is presented in a detailed and concrete way through appropriate tables and figures. Our experimental results are based on realistic scenarios and the evaluation of energy consumption for different group sizes offers a very useful insight into each protocol's scalability and practicality. We have theoretically computed the communication (in terms of the number of sent-received bits) and computation complexity of all protocols (in terms of basic cryptographic operations) and based on these complexities we computed the total energy cost. Even though our assessments are not based on actual implementations, we believe that they are indicative of the overall performance of the protocols. Our ultimate goal is to provide a reference point for future works, which can help in the discovery of new, efficient protocols.

The rest of the paper is organized as follows: in Section 2 we examine the related work, while in Section 3 we present our assumptions for the comparison of the GKA protocols. All protocols are presented in Section 4 starting from schemes requiring five (5) communication rounds and ending the section with one-round GKA protocols. Section 5 includes our analytic performance evaluation and we conclude the paper with Section 6.

2. Related work

Few papers have been presented in the literature that concern surveys on GKA protocols. The most recent work is (Klaoudatou et al., 2010), where E. Klaoudatou et al. have presented a survey on Cluster-based GKA protocols for Wireless Sensor Networks (WSNs). The comparison between the various protocols takes into account the size of the network, as well as the size of the clusters. Using these parameters the authors assess the computation and communication cost of all protocols and compare their efficiency through analytic tables and figures. We have followed the same approach in order to evaluate the performance of the examined protocols. However, the work in Klaoudatou et al. (2010) focuses on applications of WSNs in the healthcare sector and thus takes into account GKA protocols applied only on networks that can be organized in clusters. Due to this cluster-based structure, none of the presented GKA protocols requires a constant number of rounds.

In Manulis (2006), M. Manulis presented an overview of some known group key exchange protocols. He mainly focused on the security aspects of the protocols and did not provide any efficiency comparison. In Dutta and Barua (2005b), R. Dutta and R. Barua provided a complete survey on two-party, three-party and multi-party key agreement protocols. They have presented in a brief, but concrete way the communication and computation cost of each protocol, without however making any further comparison. Y. Amir et al. in (Amir et al., 2004) presented a thorough performance evaluation of five notable distributed key management techniques. Their analytic experimental results were obtained in actual local and wide area networks and they have examined not only the key establishment phase of the protocols, but also the performance of their group membership events. O. Pereira's PhD dissertation (Pereira, 2003) mainly focused on the construction of a simple model for the analysis of a classical family of authenticated GKA protocols (the Clique family). He discovered several attacks concerning this family of protocols and trying to fix these problems, he designed a new authenticated GKA protocol based on different cryptographic primitives. In his work, the new protocol is compared with the Clique family, as regards to their performance and correctness.

Beside the aforementioned works, several papers are surveying key management protocols. Clearly, the most important stage in a group key management scheme is group key agreement. In Zhang and Varadharajan (2010), J. Zhang and V. Varadharajan presented a survey on key management schemes for WSNs. In their work, the authors included several key agreement schemes presenting their computation and communication costs. The classification that takes place in (Zhang and Varadharajan, 2010) mainly concerns the computation, communication and storage complexity of the examined schemes. In Jiang and Hu (2008), the authors B. Jiang and X. Hu presented some security problems in multicast-oriented communication. They analyzed some centralized and decentralized key management protocols and discussed new research directions to group key management.

Van der Merwe et al. presented in Merwe et al. (2007) a survey on the most popular peer-to-peer key management protocols for Mobile Ad Hoc Networks (MANETs). The protocols are divided into groups based on their design strategy and main characteristics. The framework of this paper is general making it a reference point for the development of new, innovative schemes and protocols. Another work examining some recent papers concerning key management protocols in Mobile Ad Hoc Networks is (Wu et al., 2007), written by B. Wu, J. Wu and M. Cardei. The authors examined several constraints and limitations of MANETs, giving the touchwood for new research projects, concerning key management in such environments.

The relatively older work (Challal and Seba, 2005), by Y. Challal and H. Seba, examined a variety of group key management protocols, which are classified and compared, according to some pertinent performance criteria. This comparison considers the cost of re-keying, as well as the storage cost, which comes as a result of keys' accumulation. Thus, this comparison is primarily focused on communication cost. Finally, S. Rafaeli and D. Hutchison in Rafaeli and Hutchison (2003) divided the key management protocols into three main classes: centralized group key management protocols, decentralized architectures and distributed key management protocols. In their paper, the authors described the different features and goals of all these classes of protocols.

Our paper is the only survey in the literature (to the best of our knowledge) together with (Klaoudatou et al., 2010), which investigates the total energy cost of the examined protocols for different sizes of the group. In this way, our experimental results offer new insights into the scalability and practicality of the constant round GKA protocols that we examine.

3. Preliminaries

The main contribution of this paper is the assessment of the complexity of all constant round GKA protocols proposed so far in the literature. The complexity analysis of the protocols comprises the calculation of the total number of computations performed by every protocol and the number of messages exchanged by each of them. In what follows, we will denote by n the number of the members in the group. Furthermore, in many protocols there is a provision for the management of membership events, like join, leave etc. In our analysis we take into account only the key establishment phase of each protocol.

For the computation cost we only take into consideration the number of modular exponentiations, scalar multiplications and the pairings performed by all group members in each protocol. However, there are several other actions taking place during the execution of a protocol, such as hash functions, symmetric encryption and signature algorithms, which are much less energy consuming tasks compared to heavy public key calculations and we consider their cost negligible.

In addition, it is important to mention that the asymmetric encryption and signature schemes bring a non-negligible computation cost. Thus, we cannot ignore their cost, even if they are not described in detail in the examined protocol. In the case that the GKA protocol assumes the execution of a public key encryption scheme, but the authors do not mention the exact scheme, we assume in our analysis that RSA is used. When a public key signature scheme is referred in the GKA protocol but the authors give no information about it, we assume that the DSA is used. The reason that we selected these two schemes is that they are the most (in our opinion) known public key protocols for encryption and signature, correspondingly. The computation cost of RSA is one exponentiation for each encryption and one exponentiation for each decryption. The use of DSA costs one exponentiation for the signature algorithm and two exponentiations for the verification algorithm. However, many GKA protocols that we examined are based on elliptic curve cryptography. In this case, when the examined GKA protocol uses an encryption algorithm, we assume that this algorithm is the elliptic curve version of ElGamal algorithm and when an unspecified signature scheme is used, we assume that the elliptic curve DSA (ECDSA) scheme is used. The computation of the encryption scheme is two scalar multiplications for the encryption and one scalar multiplication for the decryption. The ECDSA costs one scalar multiplication for the signature generation and two scalar multiplications for the verification process[1]. Usually, the use of elliptic curve cryptography improves the efficiency of a protocol based on discrete logarithms. For example, a protocol that bases its security in the discrete logarithm problem can be transformed to an elliptic curve based protocol. However, we decided not to modify the examined protocols based on discrete logarithms, since we believe that it is more proper and fair to evaluate their performance using their original version as presented in the corresponding papers.

The communication cost refers to the number of messages transmitted and received by every entity of the group. For the calculation of the broadcast messages, we assume that each broadcast message corresponds to the transmission of one message. However, the broadcast messages are received by the whole group and consequently we assume that n messages are received when a single broadcast message is sent. In many cases, the complexity of the GKA protocol is already given by the authors. However, quite often, we had to do some extra calculations, especially if the complexity analysis was not complete, or in accordance with our assumptions. For example, authors often calculate the communication cost based only on the number of rounds required by the protocol, but in our analysis we are interested in the number of transmitted and received messages, for all nodes in the group. We would like to emphasize here that our analysis results do not differ in any aspect from those in the original papers, but they might be in some cases more elaborated and specific.

Clearly, for the assessment of the communication cost, we must know the size of the exchanged messages. In the case that the examined GKA protocol is based on finite fields F_p, we assume that a single message has size 1024 bits. When the GKA protocol is based on elliptic curve cryptography, we assume that the messages have the size of an elliptic curve point (x, y), where both x, y are equal to 160 bits. It is known that 1024-bit keys in conventional cryptosystems offer the

[1] The interested reader may find additional information on the theory of elliptic curves in Blake et al. (1999) and Silverman (1986).

same level of security as 160-bit keys in elliptic curve cryptography. In particular, in the case of elliptic curves, we can assume that the exchanged messages have size only 160 bits, since only the x coordinate is necessary for the computation of the point (x, y). In many protocols however, the exchanged messages are larger than a single elliptic curve point or an element of F_p. In this case, we will say that a message has size equal to k *single* messages whenever is as large as k elliptic curve points or k elements of F_p. For example, if a message is equal to (P, Q) where P, Q are points on an elliptic curve, then we count this message as two single messages since we defined as single message only a point on the elliptic curve.

The total energy cost of each GKA protocol is simply the sum of the computation and communication cost. Without loss of generality, we use the data provided in Tan and Teo (2006) to produce a more realistic performance evaluation. Regarding the computation energy cost, according to Tan and Teo (2006), a 133 MHz "Strong ARM" microprocessor consumes 9.1 mJ for performing a modular exponentiation, 8.8 mJ for performing a scalar multiplication and 47.0 mJ for a Tate pairing. As for the communication energy cost, according again to (Tan and Teo, 2006), an IEEE 802.11 Spectrum24 WLAN card consumes 0.66 μJ for the transmission of 1 bit and 0.31 μJ for the reception of 1 bit. The abovementioned energy costs will be used for the performance evaluation of the examined GKA protocols and are summarized in Table 1.

In the following Section, we present all the constant round GKA protocols proposed so far in the literature. The most obvious classification of the protocols is to separate them according to the required number of rounds. Therefore, we firstly analyze the protocols that require five or four rounds, then the three-round protocols followed by protocols that need two rounds and finally we complete our study with GKA schemes that require only one round for their execution. These four main categories include many protocols which can be classified also based on some important security features. All GKA protocols must at least offer security against passive attacks. If a protocol is also resistant to active attacks, then we will say that it is *authenticated*. When no authentication is added in a protocol, then we will denote it as *unauthenticated*.

The most classical way to add authentication to GKA protocols is to adopt a signature scheme. As shown in Katz and Yung (2003), this technique can be made quite general and efficient transforming any group key exchange protocol which is secure against passive adversaries into one that is secure against active ones. Such general techniques are usually called *compilers*. The adoption of a signature scheme for authentication reasons requires the use of infrastructures to handle public keys and certificates. One way to avoid them is to use passwords or IDs for authentication. In ID-based systems, the public key of a user can be calculated from his identity, while the private key can be computed on his behalf by a trusted authority, called Key Generation Center (KGC). The main advantage of ID-based and password-based key agreement protocols in comparison with certificate-based systems is the simplification of the key management procedure. However, this may come with an extra computational complexity (for example, ID-based GKA protocols require pairing operations which are quite heavy for the system).

Table 1 – Energy Costs for Computation and Communication.

Computation cost of Modular Exponentiation	9.1 mJ
Computation cost of Scalar Multiplication	8.8 mJ
Computation cost of Tate Pairing	47.0 mJ
Communication cost for transmitting a bit	0.66 μJ
Communication cost for receiving a bit	0.31 μJ

Beside these general characteristics (authenticated-unauthenticated, certificate-based – ID-based – password-based) of a GKA protocol, a very important issue is how their security attributes are proved. To this direction and in order to make the analysis of group key exchange protocols more formal, Bresson et al. (2001) introduced a formal security model. Most of the contemporary GKA protocols use this model to prove their security. In general, we say that a system is *provably secure* if its security can be proved formally in a specific model (such as Bresson et al. (2001)), where we have made assumptions on what an adversary can do and to which information has access. Finally, in the next section we will categorize the GKA protocols according to their suitability in different networks. For example, some GKA protocols are suitable for networks where the nodes have the same (or different) capabilities, are organized in a specific structure or require a hierarchy between them.

4. Constant round group key agreement protocols

In this section, we describe in brief all the constant round Group Key Agreement (GKA) protocols that have been proposed so far in the literature. We classify these protocols, mainly according to the number of rounds needed to complete their execution, but also, according to the adopted authentication mechanism, the required network structure and the general method used to obtain the common secret key of the group. For the rest of this paper, we denote by n the number of protocol participants. Furthermore, we named the protocols after the authors' initials and the year of publication. When the same authors have published two or more protocols in the same year, then we add a lowercase letter (a, b, c etc.) after the publication year.

4.1. *Five and four-round authenticated group key agreement protocols*

In this subsection, we present GKA protocols that complete their execution in five or four communication rounds. We would like to note that all of these protocols are authenticated. Section 4.1 starts with the analysis of a five-round protocol, which is based on a Trusted Third Party (TTP) for its execution. It continues with the analysis of five four-round protocols, based also on trusted entities, followed by the analysis of a four-round protocol, based on a Key Generation Center (KGC) and bilinear pairings. Finally, we examine two four-round protocols, based on hash functions. The description of those nine protocols follows.

4.1.1. *AP06 protocol (Abdalla and Pointcheval, 2006)*

In Abdalla and Pointcheval (2006), M. Abdalla and D. Pointcheval presented the first password-based Group Key Exchange protocol that was proved secure in the standard model. This protocol is based on smooth projective hash functions and it makes use of digital signatures for authentication purposes. The notion of projective hash function families was first introduced by Cramer and Shoup (2002) in order to design chosen-ciphertext secure encryption schemes. In Gennaro and Lindell (2003) the interested reader can find more information on such families together with a way to use them for building secure password-based authenticated group key exchange protocols. For the completion of this protocol, the existence of a trusted server is needed and the network nodes are disposed in a ring structure. The protocol completes its execution in five rounds and, to the best of our knowledge, this is the only five-round protocol proposed in the literature. Its computation cost is equal to $2n^2 + 6n$ modular exponentiations and its communication cost consists of $11n$ sent messages and $11n(n-1)$ received messages. The size of each message is 1024 bits.

4.1.2. *JV96 protocol (Just and Vaudenay, 1996)*

The first four-round authenticated GKA protocol, proposed in the literature, is introduced in Just and Vaudenay (1996). This protocol constitutes an extension of a key agreement protocol for two parties and for its execution the participants have to initially execute the two-party protocol. The authors compare their scheme with Burmester-Desmedt protocol (Burmester and Desmedt, 2005) and they conclude that it is more efficient than this in terms of communication. Regarding the computation cost of this protocol, it is equal to $4n$ modular exponentiations, while its communication cost is $3n$ sent messages and $n^2 + n$ received messages. The size of each message is 1024 bits.

4.1.3. *BS06 protocol (Bohli and Steinwandt, 2006)*

A four-round authenticated GKA protocol is presented in Bohli and Steinwandt (2006). This protocol provides perfect forward secrecy and it is secure against malicious insiders. The protocol relies on a TTP and it is based on the Diffie-Hellman problem. Its computation cost is $2n^2 + 2n$ modular exponentiations and its communication cost is $7n$ sent messages and $7n(n-1)$ received messages, whose size is 1024 bits.

4.1.4. *TYO07 protocol (Tso et al., 2007)*

In Tso et al. (2007), a four-round GKA protocol is presented, which is designed for dynamic peer groups in mobile computing environments. The protocol introduced in Tso et al. (2007) is based on mobile users' identities and it also uses smart cards for its execution. This protocol requires from the participants to hold a smart card containing their secret keys. This requirement can make the protocol impractical for many applications. However, it can be compared with the rest of the protocols because the structure of the scheme can be used as it is, even to environments which do not require smart cards. The proposed protocol achieves implicit group key authentication, key confirmation, forward secrecy and key independence. Two trusted entities are involved in the protocol execution, namely the card issuer and the base station. For the completion of the protocol, $2n^2 + 5n$ modular exponentiations have to be executed. In addition, $n^2 + 5n + 1$ messages have to be sent and $4n^2 + n$ messages have to be received, totally in the network. The size of each message is 1024 bits. A drawback of this protocol, concerning its performance, is the size of the sent messages in the third round, since it is equal to n single messages for each user. The large size of the messages significantly augments the communication cost. The protocol also discusses the case of a mass join/leave operation. In particular, if m is the number of members that join/leave the group, then a mass join operation requires $(n+m)^2 + 6m + 5n + 1$ exponentiations, $5n + 4m + 1$ messages should be sent and $2n^2 + 2m^2 + 4mn + 4n + 3m$ messages will be received. A mass leave operation will need $3n - 3m - 3$ exponentiations, $2n - 2m$ messages will be sent and $(n-m)(n-m+1)$ messages will be received.

4.1.5. *WRLP08 protocol (Wan et al., 2008)*

In Wan et al. (2008), an ID-based GKA protocol is proposed. Taking into account the importance of anonymity, especially in wireless networks, the authors present a protocol that besides the basic security features such as confidentiality and authentication, it also provides privacy. The concept of privacy in this work represents the ability of the system to protect the identity of the group members from outside eavesdroppers. Notice that this requirement is not always necessary in ID-based cryptosystems. In addition, the protocol does not involve enormous computational requirements, since it is designed for wireless networks, where the mobile devices have limited computational capabilities. The computation cost of the protocol is $n^2 + 5n - 3$ scalar multiplications and $2n$ pairings. As for its communication cost, it is $9n - 7$ sent messages and $2n^2 + 5n - 7$ received messages, whose size is 160 bits. Moreover, the protocol provides algorithms for the case that a member joins or leaves the group. A join operation requires 3 pairings and 19 scalar multiplications, while its communication cost is 11 sent messages and $n + 10$ received messages. A leave operation has a communication cost equal to 8 sent messages and $2n + 2$ received messages, while its computation cost is 2 pairings and $2n + 6$ scalar multiplications.

4.1.6. *FXW09 protocol (Fu et al., 2009)*

In Fu et al. (2009), a password-based authenticated GKA protocol is proposed. This protocol is provably secure and uses the passwords for authentication purposes. One of the most innovative features of this protocol is that each member in the group has a different password, in contrast to the majority of the password-based GKA protocols, where the users share a common password. Moreover, the protocol relies on a trusted entity, namely the system's server. The computation cost of this protocol is $7n$ modular exponentiations and its communication cost is $5n$ sent messages and $2n^2 + n$ received messages. The size of each message is 1024 bits. The protocol also considers the case of mass join/leave operation. According to Fu et al. (2009), a mass join operation will cost $7m + 4$ exponentiations (where m is the number of joining members), while $6m + 2n + 2$ messages will be sent and $2n^2 + m^2 + 3mn + 3m + n$ messages will be received. A mass leave operation on the other hand will require the re-execution of the whole GKA protocol.

4.1.7. Y04 protocol (Yi, 2004)

The protocol proposed in Yi (2004), is another four-round protocol, based on a KGC. This protocol is an ID-based, fault tolerant GKA protocol, which can be executed in three rounds instead of four, if no faults are detected. Its execution involves the presence of a semi-trusted bridge, which interacts with the protocol participants. The proposed protocol is based on elliptic curve cryptography and its computation cost is $2n$ exponentiations, $2n^2$ pairings and $7n$ scalar multiplications. Its communication cost is $n^2 + 3n + 1$ sent messages and $3n^2 + 2n$ received messages, while the size of each message is 160 bits. Both the computation and the communication cost of this protocol are calculated under the assumption that no faults are detected. This protocol's total energy cost is highly affected by the fact that during the second round, each user has to perform $n - 1$ pairings. In addition, the second round's message size, sent by each user is equal to $n + 1$, which really augments the communication cost of the protocol in question.

4.1.8. ABCP06 protocol (Abdalla et al., 2006)

An authenticated, password-based four-round GKA protocol is proposed in Abdalla et al. (2006). This protocol is based on Burmester-Desmedt (BD) protocol (Burmester and Desmedt, 2005) and it is provably secure in the random oracle and ideal cipher models, under the Decisional Diffie-Hellman assumption. The authors have added authentication using passwords in the original BD protocol, with the cost of adding two more rounds on it. The total computation cost of ABCP06 (Abdalla et al., 2006) is $3n$ modular exponentiations, while its total communication cost is $4n$ sent messages and $4n(n - 1)$ received messages. Each message has size equal to 1024 bits.

4.1.9. ZZLC09 protocol (Zheng et al., 2009)

Finally, another four-round protocol is presented in Zheng et al. (2009). This protocol shares many common attributes with the protocol proposed in Abdalla et al. (2006), as they fulfill the same security requirements and they are both password-based. The authors of Zheng et al. (2009) analyze the security of their protocol by conducting several experiments and presenting the corresponding results. The computation cost of this protocol is $5n$ modular exponentiations, while its communication cost is $4n$ sent messages and $4n(n - 1)$ received messages. The size of each message is 1024 bits.

4.2. Three-round group key agreement protocols

In this subsection, we examine the GKA protocols that require three rounds to complete their execution. Firstly, we present eight protocols that provide authentication. The first is a hierarchical protocol, while the following two are based on KGCs and pairing-based cryptography. The following two protocols come from the same paper and are based on a TTP. Next, we examine two protocols based on hash functions, followed by a protocol based on the different computational capabilities of network nodes. Finally, the last authenticated three-round protocol we examine is based on a group leader. Beside these eight protocols, this subsection also analyzes the performance of two more GKA protocols that are presented in the corresponding papers in both an authenticated and an unauthenticated version.

Finally, we would like to mention that a password-based group key exchange protocol is presented in Wu and Zhu (2008), which also requires three rounds. This protocol is generic in the sense that it can transform any password-based authenticated key exchange protocol between *two* parties to a password-based authenticated *group* key exchange protocol. The first round requires the execution of the two-party protocol and then two more rounds are needed for the construction of the final group key. Clearly, the assessment of the efficiency of the group key exchange protocol is based on the performance of the two-party protocol and for this reason the generic scheme presented in Wu and Zhu (2008) is not included in our analysis.

4.2.1. Authenticated protocols

4.2.1.1. NKYW04 protocol (Nam et al., 2004c). In Nam et al. (2004), an authenticated three-round GKA protocol is proposed, based on a hierarchical tree structure. The protocol divides the network nodes into powerful nodes and low-power nodes. Although the protocol is hierarchical, which constitutes a general case of non-constant round protocols, the proposal remains constant round, since the tree levels are only three, regardless of the number of protocol participants. In this paper, the authors use as a basis for their proposal a two-round protocol for two parties. The generalized version of this protocol constitutes the final three-round GKA protocol. Apart from the total number of protocol participants, denoted by n, this protocol also makes use of a parameter m, which denotes the number of high performance network nodes. For our experimental assessments we have chosen the value of m being equal to (according to the authors of Nam et al. (2004)) the largest positive integer such that $m^2 \le n - 1$. For example, if $n = 125$ then $m = 11$. The computation cost of the protocol is equal to $mn - m^2 + 2m + 3n + 1$ modular exponentiations. The communication cost of the protocol is $n + 2m + 1$ sent messages and $3\ nm + 3n - m - 3$ received messages, while each message has size 1024 bits.

4.2.1.2. PHYK08 protocol (Park et al., 2008). In Park et al. (2008), the authors proposed an improved version of the protocol presented in Choi et al. (2004). The protocol proposed in Park et al. (2008) has been improved regarding some security attributes compared to Choi et al. (2004), since it is fully authenticated and it is resistant to replay attacks. However, for the enhancement of these security issues, the KGC involved in the execution of the protocol needs to be always active and online. The protocol's computation cost is $9n$ scalar multiplications and $2n + 2$ pairings. As for its communication cost, it is $4n$ sent messages and $n^2 + 2n$ received messages. The size of each message is 160 bits.

4.2.1.3. YWJ08 protocol (Yao et al., 2008). Another authenticated three-round GKA protocol based on the notion of identity-based cryptography is proposed in Yao et al. (2008). The first round of the protocol serves as the identity authentication round, in the second round the key agreement takes place and the last round is necessary for the satisfaction of the key confirmation property. Moreover, the protocol is provably secure in the random oracle model. Its computation cost is $2n^2 + 4n$ scalar multiplications and $n^2 + 5n$ pairings. Regarding the communication cost, it is equal to $5n$ sent messages and $5n(n - 1)$ received messages, whose size is 160 bits.

4.2.1.4. *YHVK08 protocols (Yeun et al., 2008)*. The work of Yeun et al. (2008) sets some additional security requirements for GKA protocols, in order to make them more suitable for dynamic MANET environments. In particular, in Yeun et al. (2008) an improved version of Burmester-Desmedt protocol (Burmester and Desmedt, 2005) and Choi et al.'s protocol (Choi et al., 2004) are proposed. These improved protocols are able to detect and identify malicious insiders in mobile ad-hoc networks and their structure is closely related to the original ones. Regarding the enhanced version of Burmester-Desmedt protocol (denoted by YHVK08 (1)), it brings a computation cost of $4n^2 + 6n$ modular exponentiations and a communication cost of $6n$ sent and $6n(n - 1)$ received messages, whose size is 1024 bits. The enhanced version of Choi et al. protocol (denoted by YHVK08 (2)) has a computation cost equal to $4n^2 + 6n$ scalar multiplications and $4n$ pairings. The communication cost of the latter protocol comes to $6n$ sent and $6n(n - 1)$ received messages, while the size of each message is 160 bits.

4.2.1.5. *BC04a protocol (Bresson and Catalano, 2004a)*. The papers Bresson and Catalano (2004a) and Bresson and Catalano (2004b) actually propose the same three-round authenticated GKA protocol. In their second work, the authors provide some additional definitions regarding the protocol's proof of security and they also propose a general model, which can serve as the basis for the generation of new three-round GKA protocols. For authentication purposes, the proposed protocol uses an asymmetric digital signature scheme. The computation cost of the protocol is $8n^2 - 3n$ exponentiations, while its communication cost is $5n^2 - 3n$ sent messages and $7n(n - 1)$ received messages. The size of each message is 1024 bits.

4.2.1.6. *BVS06 protocol (Bohli et al., 2006b)*. In Bohli et al. (2006b), a password-based authenticated, provably secure GKA protocol is proposed. This protocol uses the notion of smooth projective hashing and its security is based on the common reference string model. In particular, the protocol builds on a non-interactive non-malleable commitment schemes and a smooth projecting hash family. Since the ideas behind this protocol are diametrically different from the notions of all other examined GKA protocols in this paper (e.g. they cannot be directly compared to exponentiations or scalar multiplication operations), we cannot precisely evaluate the protocol's efficiency and thus it is excluded from our comparison.

4.2.1.7. *NLKW05 protocol (Nam et al., 2005)*. In (Nam et al. (2005), two versions of the same GKA protocol are presented: the first is secure against active attacks and the second is secure against passive attacks. The primary contribution of Nam et al. (2005) is the authenticated, three-round protocol while the unauthenticated protocol is a two-round protocol that constitutes the basic part of the former protocol. Both protocols are provably secure under the decisional Diffie-Hellman assumption and are applicable in an asymmetric environment, where the powerful application server takes much of the computational burden from the mobile devices. The computation cost of the three-round protocol is $8n - 4$ exponentiations. The communication cost of this protocol is $4n - 1$ sent messages and $2n^2 + n - 3$ received messages, while the size of each message is 1024 bits.

4.2.1.8. *ABIS07 protocol (Augot et al., 2007)*. Another three-round authenticated GKA protocol, particularly well suited for MANETs, is ABIS07 (Augot et al., 2007). The protocol is provably secure against active adversaries. The authors of Augot et al. (2007) adopt the concept of "current leader", which is a network node charged with relatively higher computational and communication tasks and it is chosen before the execution of each session. The computation cost of the protocol is $10n - 8$ exponentiations and its communication cost is $6n$ sent messages and $3n^2$ received messages. The size of each exchanged message is 1024 bits.

4.2.2. *Authenticated and unauthenticated protocols*

In this subsection, we present two three-round GKA protocols, which have been presented in both their authenticated and unauthenticated version. Since the unauthenticated version is the basis for the authenticated one, the unauthenticated protocols are more efficient in terms of computation and usually also in terms of communication.

4.2.2.1. *HLL07 protocols (Hu et al., 2007)*. In Hu et al. (2007), two GKA protocols, based on bilinear pairings, are proposed. The unauthenticated protocol completes its execution in two rounds, while the authenticated protocol requires three rounds. These protocols are designed for asymmetric networks, comprising by nodes with different computational capabilities. In particular, one node has very high computational capabilities and all other nodes have limited computational capabilities. Due to the slight differences between the authenticated and the unauthenticated version of the protocol, only the authenticated version is going to be evaluated. Hence, the computation cost of the authenticated protocol is $2n^2 + 6n - 4$ scalar multiplications and $2(n - 1)$ pairings. Regarding the communication cost of the protocol, it is equal to $4n + 2$ sent messages and $4n^2 - 4$ received messages. The size of each message is 160 bits.

4.2.2.2. *NPKW07 protocols (Nam et al., 2007)*. The authors of Nam et al. (2007) propose two GKA protocols, which provide perfect forward secrecy and have logarithmic computational complexity. The unauthenticated version of the protocol, even though it serves as the basis for the authenticated one, it is not a GKA protocol, but a Key Distribution Protocol. Regarding the authenticated protocol, it is based on a tree structure considered among the participants of the group and also uses digital signatures to achieve authentication. We assessed the energy cost of this protocol considering a balanced tree structure, since the majority of the hierarchical protocols require such structure. In this case, the computation cost of the protocol in question is $5n + n/2 + 5n \log n - 1$ modular exponentiations. As for the communication cost of the protocol, it is $5n - 2$ sent messages and $2n + 10n \log n - 2$ received messages. The size of each message is 1024 bits. It is also worth mentioning, that the group key depends primarily on the root of the tree structure and it is not derived in a fully contributory way.

4.3. *Two-round group key agreement protocols*

The majority of the constant round GKA protocols require two rounds. Our research has led us to forty-nine (49) protocols. Initially, we present the thirty-one authenticated protocols, which are divided into four categories. After the analysis of the authenticated protocols, we examine unauthenticated two-round GKA protocols (ten protocols in total). Finally, we present eight protocols having an authenticated and an unauthenticated version.

4.3.1. *Authenticated protocols*

Most of the constant round GKA protocols presented in the literature so far are authenticated two-round protocols. Thus, we divided them into the following categories, in order to compare them more easily. Initially, we present the protocols based on a Certification Authority (CA) or on a Trusted Third Party (TTP), which are four and two protocols, respectively. To continue, we present thirteen protocols based on bilinear pairings[2]. Next, we examine five authenticated two-round GKA protocols, which are based on the different computational capabilities of network nodes. Finally, the authenticated two-round protocols' subsection is completed with seven more protocols based on hash functions. It is worth mentioning that there is one more two-round authenticated protocol, proposed in Zou et al. (2006) (ZTR06), but since this protocol is proposed in the same paper along with a one-round protocol, we present it in the Section of one-round protocols (Section 4.4). However, we have compared it, regarding its performance, with authenticated two-round protocols in Section 5.4.

4.3.1.1. *Authenticated protocols based on certification authorities or other trusted parties.*

4.3.1.1.1. T05b protocol (Tseng, 2005b). In Tseng (2005b), a two-round authenticated GKA protocol is proposed. This protocol offers forward secrecy and it is provably secure against passive attacks in the random oracle model, under the decisional Diffie-Hellman problem. In addition, the protocol in question is fault tolerant. For authentication purposes, the protocol in Tseng (2005b) uses digital certificates. The computation cost of the protocol is $9n^2 - 5n$ exponentiations, while its communication cost is $n^2 + 5n$ sent messages and $n^3 + 4n^2 - 5n$ received messages, whose size is 1024 bits. This protocol has a cubic number of received messages due to the second round's broadcast message. The size of this broadcast message, sent by every group member, is equal to $n + 2$ single messages; hence, the cost of this round only is $n(n + 2)$ sent messages and $n(n + 2)(n - 1)$ received messages.

4.3.1.1.2. T07a protocol (Tseng, 2007a). Another two-round GKA protocol, which has slight differences with the abovementioned T05b protocol (Tseng, 2005b), is presented in Tseng (2007a). The security features of Tseng (2005b) are the same also for T07a protocol. However, the latter offers security against known-key attacks and it is more efficient than the former, since it requires the transmission of fixed-size messages for each participant of the protocol. The computation cost of the protocol in Tseng (2007a) is slightly lower than the corresponding cost of Tseng (2005b), since it is equal to $8n^2 - 2n$ exponentiations. Regarding its communication cost, it is significantly reduced compared to Tseng (2005b), being equal to $8n$ sent messages and $8n(n - 1)$ received messages. The size of each message is 1024 bits. Moreover, the protocol provides algorithms for the case that a member joins or leaves the group. A join operation requires $5n + 12$ exponentiations and its communication cost is $4n + 13$ sent messages and $19n - 2$ received messages. A leave operation has a communication cost equal to 8 sent messages and $8(n - 2)$ received messages, while its computation cost is $n + 5$ exponentiations.

4.3.1.1.3. ZWZ07 protocol (Zheng et al., 2007). The protocol proposed in Zheng et al. (2007) requires the existence of a Certification Authority for authentication purposes. This protocol is well suited for dynamic peer groups and wireless environments, such as MANETs. The protocol is based on ElGamal encryption and signature schemes. According to its description, the computation cost is equal to $2n^2 + 3n$ modular exponentiations and the communication cost of the protocol is $n^2 + 5n$ sent messages and $n^3 + 4n^2 - 5n$ received messages, whose size is 1024 bits. It is worth mentioning that this protocol exhibits a significant performance drawback, which is the second round's broadcast message size. The number of messages to be sent during the second round is $n(n + 3)$, while the number of messages to be received totally in the network is $n(n + 3)(n - 1)$. Finally, we would like to note that the protocol also takes consideration of join and leave operations. In particular, the computation cost of a member's join operation is $2n + 3$ exponentiations, while the corresponding cost for a leave operation is $2n - 2$ exponentiations. The communication cost will be equal to $4n + 11$ sent messages and $4n^2 + 10n - 4$ received messages for a join operation, and $3n + 1$ sent messages and $3n^2 - 5n - 2$ received messages for a leave operation.

4.3.1.1.4. ZWZL09 protocol (Zhang et al., 2009). Another two-round GKA protocol based on a Certification Authority is proposed in Zhang et al. (2009). The main difference between this protocol and the rest of the protocols of this class is that it does not require hash functions. The protocol is provably secure and its security reduces to the decisional Diffie-Hellman assumption. The computation cost of this protocol is $4n^2 - n$ exponentiations. The communication cost of the protocol is $6n$ sent messages and $6n(n - 1)$ received messages, while the size of every message is 1024 bits.

[2] The interested reader may refer to Avanzi et al. (2006) and Dutta et al. (2004) for more details on pairing-based cryptography.

4.3.1.1.5. BGS06 protocol (Bohli et al., 2006a). A provably secure GKA protocol based on Group Theory is proposed in Bohli et al. (2006a). The protocol provides perfect forward secrecy and it is secure against insider attacks. Apart from using hash functions, the protocol is based on automorphisms on non-abelian groups, which in fact makes this protocol so special, since no other constant round GKA protocol uses them. Taking into account these special features, which cannot be directly compared to exponentiations or scalar multiplication operations, we conclude that we cannot precisely evaluate the protocol's efficiency. Thus its performance evaluation is excluded from our comparison.

4.3.1.1.6. ZTR06 protocol (Zou et al., 2006). In Zou et al. (2006), a two-round authenticated GKA protocol based on the Chinese Remainder Theorem (CRT) is proposed. This protocol is a modified version of the scheme presented in Balachandran et al. (2005). The authors discuss the weaknesses of Balachandran et al. (2005) and propose an authenticated variant of it. The computation cost of the protocol in Zou et al. (2006) is $n^2 + 3n$ modular exponentiations. The communication cost of the protocol is $6n$ sent and $6n(n-1)$ received messages. Each message has size 1024 bits.

4.3.1.2. *Authenticated protocols based on bilinear Pairings.*

4.3.1.2.1. DWGW03a (Du et al., 2003a) and DWGW03b (Du et al., 2003b) protocols. In Du et al. (2003a), a two-round GKA protocol is proposed, which is based on an Identity-based Public Key Infrastructure (ID-PKI). This protocol is based on Burmester-Desmedt (BD) protocol (Burmester and Desmedt, 2005) and manages to add authentication on it by using a special signature scheme. The computation cost of DWGW03a (Du et al., 2003a) is $n^2 + 4n$ scalar multiplications and $4n$ pairings. Regarding its communication cost, it is equal to $3n$ sent messages and $3n(n-1)$ received messages. The size of each message is 160 bits. The protocol proposed in Du et al. (2003a) proved to be vulnerable to an impersonation attack and its authors created an improved version of the protocol in question, which could resist this attack. The improved protocol is DWGW03b (Du et al., 2003b) and it is fully authenticated. Regarding the energy cost of the latter protocol it is only burdened by one additional scalar multiplication per user. Thus the computation cost of DWGW03b (Du et al., 2003b) is $n^2 + 5n$ scalar multiplications and $4n$ pairings and its communication cost is equal to the one of the original protocol. In our performance evaluation we have included only DWGW03b (Du et al., 2003b) protocol, since both protocols bring a very similar energy cost.

4.3.1.2.2. LJY05 protocol (Li et al., 2005). Another two-round authenticated GKA protocol, based on ID-PKI, is presented in Li et al. (2005). The exchanged messages are authenticated by the use of a signature algorithm in the first round and by an HMAC operation in the second round. The computation cost of this protocol is $7n$ scalar multiplications. As for the communication cost of the protocol, it is $9n$ sent messages and $3n^2 + 3n$ received messages, while the size of each message is 160 bits. The protocol also treats the case of mass join/leave operations. Specifically, a mass join operation will require $5m + 6$ scalar multiplications (where m is the number of joining/leaving members) and its communication cost will be equal to $7(m + 2)$ sent messages and $3m^2 + 3mn + 9m + 6n + 6$ received messages. The cost of a mass leave operation is equal to $10m$ scalar multiplications, while $10m + 2n$ messages will be sent and $2n^2 - 4m^2 + 2mn - 2n + 2m$ messages will be received.

4.3.1.2.3. KNKW05 protocol (Kim et al., 2005). In Kim et al. (2005), an authenticated GKA protocol suitable for Pay-TV systems is presented. According to the authors, the previously proposed protocols, especially suited for Pay-TV systems are not applicable in practice. Thus, they present a new and efficient protocol for Pay-TV systems, which is also well suited for Internet stock quotes in mobile environments, audio and music deliveries, software updates and so forth. The computation cost of this protocol is equal to $n - 1$ modular exponentiations, $4n - 1$ scalar multiplications and $3n - 2$ pairings. The communication cost of the protocol is $3n - 1$ sent messages and $n^2 + 2n - 3$ received messages, while the size of each message is 160 bits. The communication efficiency of protocol KNKW05 (Kim et al., 2005) is significantly reduced by the second round's broadcast message, which has size equal to $n + 1$ single messages.

4.3.1.2.4. CSCW07 protocol (Cho et al., 2007). In Cho et al. (2007), a GKA protocol based on bilinear pairings is presented, especially suitable for dynamically changing groups. The proposed protocol has comparatively small computation cost, mainly due to the use of batch verification techniques in the signature scheme. This protocol is provably secure in the random oracle model, under the bilinear Diffie-Hellman assumption. The computation cost of the protocol is $3(n-1)$ modular exponentiations, $4n$ scalar multiplications and $5n - 4$ pairings. The communication cost of the protocol is equal to $4n - 1$ sent messages and $n^2 + 4n - 5$ received messages. The size of each message is 160 bits. It is worth mentioning that this protocol's communication cost is significantly burdened by the second round's broadcast message, whose size is equal to $n + 2$ single messages and increases largely the communication complexity. The authors in Cho et al. (2007) discuss also the treatment of mass join/leave operations. If we denote by m the number of join/leave members, then a mass join operation will cost $n + 3m - 1$ exponentiations, $n + 5m - 1$ pairings, $2n + 4m$ scalar multiplications, while $n + 4m + 2$ messages should be sent and $n^2 + m^2 + 2\,nm + n + 4m + 2$ messages will be received. A mass leave operation will cost $n - m - 1$ exponentiations, $n - m - 1$ pairings, $2n - 2m - 1$ scalar multiplications, while $n - m + 2$ messages should be sent and $(n - m + 2)(n - m - 1)$ messages will be received.

4.3.1.2.5. HLH07 protocol (He et al., 2007). In He et al. (2007), the authors propose a two-round GKA protocol, resistant to several known attacks, such as key exposure attacks and insider impersonation attacks. This protocol is an ID-based variant of the Burmester-Desmedt protocol (Burmester and Desmedt, 2005), offering authentication and resistance to active attacks. The computation cost of the protocol is $2n^2 + 3n$ scalar multiplications and $2n^2$ pairings. The communication cost of the protocol is $3n$ sent messages and $3n(n-1)$ received messages. The size of each message is 160 bits. During the Key Generation phase of this protocol and for authentication purposes, the protocol participants need to compute a large number of pairings and scalar multiplications, which increases the computational complexity of the protocol.

4.3.1.2.6. TZZ08 protocol (Tang et al., 2008). Combining the merits of the ID-based authenticated two-party protocol of McCullagh and Barreto (2005), along with those of Burmester-Desmedt protocol (Burmester and Desmedt, 2005), the authors of Tang et al. (2008) proposed a new ID-based authenticated GKA protocol. The computation cost of the protocol is $5n$ scalar multiplications and $3n$ pairings. Regarding the communication cost of this protocol, it is $3n$ sent messages and $n^2 + n$ received messages. The size of each message is 160 bits.

4.3.1.2.7. CHL08 protocol (Choi et al., 2008). A very efficient ID-based GKA protocol was presented in Choi et al. (2004). However, the protocol proved to be vulnerable to insider attacks and it was shown that failed to provide authentication by Zhang and Chen (2004). The authors, few years later, have provided a new ID-based protocol that overcame these security faults in Choi et al. (2008). The vulnerability to insider attacks was treated with the use of ID-based signatures. The computation cost of the protocol in Choi et al. (2008) is $n^2 + 10n$ scalar multiplications and $6n$ pairings. Regarding its communication cost, it is $5n$ sent messages and $5n(n - 1)$ received messages. The size of each message is 160 bits.

4.3.1.2.8. CM08 protocol (Cao and Ma, 2008). In Cao and Ma (2008), an ID-based GKA protocol is proposed, which provides perfect forward secrecy and it is provably secure under the standard model. In contrast to the majority of the proposed protocols, CM08 (Cao and Ma, 2008) does not require an online KGC during the execution of the protocol. The proposed protocol's computation cost is $2n^2 + 2n$ scalar multiplications and $2n$ pairings. The communication cost of the protocol is $n^2 + n$ sent messages and $n^3 - n$ received messages, whose size is 160 bits. It is obvious from the protocol description, that the second round's broadcast message is so large, that it makes the protocol in question inefficient in terms of communication, since for this round n^2 messages have to be sent and $n^2(n - 1)$ messages have to be received.

4.3.1.2.9. LTL08 protocol (Li et al., 2008). Another ID-based GKA protocol is presented in Li et al. (2008). Even though the authors claim that their protocol requires one round only, an extra round is necessary. This extra round involves a pairwise key agreement phase between all group members. For the energy cost assessment of this protocol, we assume that the pair-wise key agreement consists the first round of the protocol and consequently, the protocol does not require only one round, but two. The proposed protocol also provides perfect forward secrecy, while it does not require the computation of digital signatures. The computation cost of the protocol is equal to n^2 modular exponentiations, $3n^2 - n$ scalar multiplications and $n^2 + n$ pairings. Regarding its communication cost, it is $2n(n - 1)$ sent and $2n(n - 1)$ received messages, which have size 160 bits.

4.3.1.2.10. GZG09 protocol (Geng et al., 2009). The GKA protocol in Geng et al. (2009) is based on Certificateless Public Key Infrastructure. This protocol satisfies strong security requirements, such as key authentication, known session key security, key compromise impersonation resilience and perfect forward secrecy. The authentication is provided by the use of a certificateless signature scheme. The computation cost is equal to $7n^2 - 5n$ scalar multiplications and $4n$ pairings. Regarding the communication cost of the protocol, it is $3n^2 - 2n$ sent and $4n(n - 1)$ received messages. The size of each exchanged message is 160 bits. Similarly to the above-mentioned LTL08 protocol (Li et al., 2008), GZG09 protocol (Geng et al., 2009) requires in the first round a pair-wise communication between all participants, which consists a significant drawback for its efficiency.

4.3.1.2.11. PAK09 protocol (Park et al., 2009). The protocol in Park et al. (2009) is an improved version of Zhou et al. protocol (Zhou et al., 2006). In this work, malicious users can no longer impersonate other participants even if they know their ephemeral group secret key. Moreover, the new protocol is more efficient than Zhou et al. (2006), in terms of computation. The computation cost of PAK09 (Park et al., 2009) is $6n$ scalar multiplications and $4n - 2$ pairings. The communication cost of the protocol is $3n$ sent messages and $3n^2 - n - 2$ received messages, while the size of every message is 160 bits. Despite the fact that the examined protocol is efficient enough, its main drawback (affecting its communication cost) is that in the first round the initiator of the protocol broadcasts a very large message, equal to $n + 2$ single messages.

4.3.1.2.12. LL10 protocol (Lv and Li, 2010). The main disadvantage of ID-based authentication mechanisms is that the KGC must send users' private keys over secure channels, making private key's distribution difficult. In order to overcome this barrier, a GKA protocol based on bilinear maps, which additionally does not require secure channels for its execution, is presented in Lv and Li (2010). Although the protocol in question involves a KGC, the participants' private keys are created collaboratively and only the legitimate users know them. The computation cost of this protocol is $10n$ scalar multiplications and $5n$ pairings. Its communication cost is equal to $3n$ sent messages and $3n(n - 1)$ received messages. The size of each message is 160 bits. LL10 protocol also considers the treatment of a member's join/leave operation. The computation cost when a new member joins the group is 2 pairings and 2 scalar multiplications, while the corresponding communication cost is equal to $n + 3$ sent messages and $n^2 + n + 2$ received messages. The cost of a leave operation is 4 pairings, 4 scalar multiplications, while $n - 1$ messages should be sent and $(n - 1)(n - 2)$ messages will be received.

4.3.1.3. Authenticated protocols based on the different computational capabilities of Network nodes.

4.3.1.3.1. NKKW04 protocol (Nam et al., 2004b). An authenticated GKA protocol for high-delay wide area networks is presented in Nam et al. (2004). The proposed scheme is efficient in terms of communication and treats membership events in a constant number of rounds. The protocol is provably secure in the random oracle model and it also provides perfect forward secrecy. The total computation cost of the protocol is $8n - 6$ modular exponentiations. The communication cost is $4n - 2$ sent messages and $2n^2 - 2$ received messages, while the size of each message is 1024 bits. For the protocol execution, there is an entity, namely the group controller, which during the second round broadcasts a large message whose size is equal to $2n$ single messages. This fact significantly augments the communication cost of the protocol, increasing by a linear factor the communication complexity of the protocol. The protocol also discusses the case of a mass join/leave operation. In particular, if m is the number of members that join/leave the group, then a mass join operation requires $8m + 3n - 1$ exponentiations, $4m + 2$ messages should be sent and $2m^2 + 2mn + 2n + 2m - 2$ messages will be received. A mass leave operation will need $3n - 3m - 1$ exponentiations, $n - m + 3$ messages will be sent and $(n - m + 3)(n - m - 1)$ messages will be received.

4.3.1.3.2. *CNKW05 protocol (Cho et al., 2005)*. In Cho et al. (2005), a two-round authenticated GKA protocol, especially designed for mobile environments, is proposed. The architecture of mobile nodes is asymmetric, meaning that the protocol participants have different computational capabilities. The protocol involves a stationary server, with sufficient computational capabilities and a group of mobile devices, with limited computational capabilities. The proposed protocol is provably secure against passive attacks in the random oracle model. The computation cost of this protocol is $8n - 5$ modular exponentiations. The communication cost of the protocol is $3n$ sent messages and $n^2 + 3n - 4$ received messages. The size of each message is 1024 bits. The authors also provide algorithms for the treatment of mass join and mass leave operations. If m denotes the number of join/leave members, then the computation and communication cost of mass join operation is $3n + 8m - 2$ exponentiations and $n + 3m + 2$ sent and $n^2 + m^2 + 3\,nm + n + 3m - 2$ received messages respectively. For mass leave operations the total computation and communication cost is $3n - 3m - 2$ exponentiations and $n - m + 2$ sent and $(n - m + 2)\,(n - m - 1)$ received messages respectively.

4.3.1.3.3. *T07c protocol (Tseng, 2007c)*. A GKA protocol for an asymmetric and mobile network is presented in Tseng (2007c). An asymmetric network consists of many mobile nodes with limited computing capability and a powerful node with less restriction. The protocol is provably secure against passive attacks and impersonation attacks. Moreover, it provides forward secrecy and implicit key authentication. The computation cost of this protocol is equal to $6n - 4$ exponentiations. Its communication cost is $4n - 3$ sent messages and $2n^2 - n - 1$ received messages, whose size is equal to 1024 bits.

4.3.1.3.4. *LWH09 protocol (Lu et al., 2009)*. The protocol proposed in Lu et al. (2009) is another authenticated GKA protocol, which bases its security on the Elliptic Curve Discrete Logarithm Problem (ECDLP). Some of the most important security features of the protocol are that it achieves mutual authentication, forward secrecy, while it is resistant against impersonation attacks. The execution of the protocol involves three different types of participants: the System Authority, the low-power nodes and a powerful node. The computation cost of the key agreement protocol is $9n + 1$ scalar multiplications. The communication cost of the protocol is $7n + 3$ sent and $3n^2 + 7n - 6$ received messages, while the size of each message is 160 bits. Moreover, the protocol provides algorithms for the case that a member joins or leaves the group. A join operation requires $2n + 10$ scalar multiplications and its communication cost is $2n + 7$ sent messages and $2n^2 + 4n + 3$ received messages. A leave operation has a communication cost equal to $2n + 1$ sent messages and $(2n + 1)(n - 2)$ received messages, while its computation cost is $2n - 2$ scalar multiplications.

4.3.1.3.5. *SC09 protocol (Saha and Chowdhury, 2009a)*. In Saha and Chowdhury (2009a) and Saha and Chowdhury (2009b), the same GKA protocol is presented. This protocol is designed for asymmetric or heterogeneous environments, where the network nodes have different computational capabilities. In the latter work Saha and Chowdhury (2009a), the generation algorithm of the polynomial used for the execution of the protocol is presented in more detail. Moreover, in Saha and Chowdhury (2009a), a more complete security analysis of the proposed protocol is provided. An important feature of this protocol is that it uses a counter, in order to avoid replay attacks (instead of timestamps that are usually used). This feature enables the offline execution of some parts of the protocol, which gives the opportunity to reduce the energy cost of the protocol in question. The computation cost of the protocol is $7n - 6$ modular exponentiations. As for the communication cost of the protocol, it is equal to $3n - 2$ sent messages and $n^2 + n - 2$ received messages. The size of each message is 1024 bits. Although the protocol in question is a very efficient protocol, the second round's broadcast message sent by the powerful node U_0 is very large, comprising by n single messages; a fact which significantly augments the communication cost of the protocol. If that broadcast message was not that large, the communication complexity of SC09 (Saha and Chowdhury, 2009a), would be linear. Finally, we would like to note that the protocol also takes consideration of join and leave operations. In particular, the computation cost of a member's join operation is $2n + 6$ exponentiations, while the corresponding cost for a leave operation is $2n - 3$ exponentiations. The communication cost will be equal to $n + 2$ sent messages and $n^2 + n + 1$ received messages for a join operation, and n sent messages and $n^2 - 2n$ received messages for a leave operation.

4.3.1.4. *Authenticated protocols based on hash functions.*

4.3.1.4.1. *KLL04 protocol (Kim et al., 2004a)*. In Kim et al. (2004), a dynamic GKA protocol is presented especially suited for MANETs. The goal of this paper is not only to provide a constant round GKA protocol, but also to treat membership events as efficiently as possible. The protocol's computation cost is $4n^2 + n$ modular exponentiations. The communication cost of this protocol is $5n$ sent messages and $5n(n - 1)$ received messages. The size of each message is 1024 bits. The protocol also discusses the case of a mass join/leave operation. In particular, if m is the number of members that join/leave the group, then a mass join operation requires

$4m^2 + 4mn + m + 1$ exponentiations, $4m$ messages should be sent and $4m(n + m - 1)$ messages will be received. A mass leave operation will need $2n^2 - 2m^2 + 5m - n$ exponentiations, $2n + 2m$ messages will be sent and $2(m + n)(n - m - 1)$ messages will be received.

4.3.1.4.2. *LHL04 protocol (Lee et al., 2004)*. A computationally efficient password-based GKA protocol is presented in Lee et al. (2004). The proposed protocol is authenticated and provably secure in the random oracle and in the ideal cipher model. It also provides forward secrecy. The computation cost of this protocol is $3n$ modular exponentiations. As for its communication cost, it is $2n$ sent messages and $2n(n - 1)$ received messages, whose size is 1024 bits.

4.3.1.4.3. *TT05 protocol (Tan and Teo, 2005)*. An authenticated variant of Burmester-Desmedt (BD) protocol (Burmester and Desmedt, 2005) is presented in Tan and Teo (2005). The protocol is also based on the Schnorr signature scheme (Schnorr, 1991) and every user should generate and verify only one signature during the execution of the protocol, which allows the computational complexity to remain linear. Beside the computation efficiency, the protocol does not increase the number of rounds of Burmester-Desmedt protocol (Burmester and Desmedt, 2005), which is usually the case in every authenticated variant of it. The computation cost of this protocol is $8n$ modular exponentiations. The communication cost of the protocol is $5n$ sent messages and $5n(n - 1)$ received messages. The size of each message is 1024 bits.

4.3.1.4.4. *CKE06 protocol (Cho et al., 2006)*. Another GKA scheme, especially designed for mobile agents in e-Commerce applications, is proposed in Cho et al. (2006). This scheme is actually based on a special type of function, namely Strong Associative One-Way Function (Strong-AOWF). The e-Commerce system described in Cho et al. (2006) is an Internet platform, where purchases and sales of products, together with the corresponding services are taking place. The agents are elements of autonomous software, searching on behalf of the buyer for the most suitable offer, according to the buyer's preferences. The search concludes to a final suggestion, according to the comparisons done by the mobile agents. For the proper execution of this platform, the GKA scheme has to be implemented among the agents. For its completion, symmetric encryptions-decryptions have to take place, as well as the aforementioned Strong-AOWF. Since no other computations are executed for this GKA scheme, we cannot directly compare it with the rest of the examined protocols and consequently, protocol CKE06 (Cho et al., 2006) is excluded from the performance evaluation of this paper.

4.3.1.4.5. *DB06 protocol (Dutta and Barua, 2006)*. Another password-based authenticated GKA protocol, secure against dictionary attacks, is presented in Dutta and Barua (2006). The proposed protocol is based on KLL04 protocol (Kim et al., 2004a). In particular, the authors have transformed the authenticated version of KLL04 protocol into a password-based authenticated GKA protocol, which they have proved that it is provably secure in the random oracle and the ideal cipher model. Protocol DB06 (Dutta and Barua, 2006) uses symmetric, password-based encryption for the exchanged messages, which constitutes the main difference it has with protocol KLL04 (Kim et al., 2004a). In addition, protocol DB06 (Dutta and Barua, 2006), contrarily to protocol KLL04 (Kim et al., 2004a), does not require the use of digital signatures schemes. The computation cost of DB06 (Dutta and Barua, 2006) is $3n$ exponentiations, while its communication cost is $3n$ sent messages and $n^2 + n$ received messages. Each exchanged message has size 1024 bits.

4.3.1.4.6. *KJL06 protocol (Kwon et al., 2006)*. The first provably secure password-based authenticated group key exchange protocol in the standard model is presented in Kwon et al. (2006). The main advantage of this protocol is that compared to the majority of password-based GKA protocols, it achieves a constant number of communication rounds. Its computation cost is $6n$ exponentiations, while the communication cost is equal to $2n$ sent messages and $2n(n - 1)$ received messages. The size of each message is 1024 bits.

4.3.1.4.7. *FWM08 protocol (Feng et al., 2008)*. Another two-round authenticated GKA protocol, suitable for mobile ad hoc environments, is presented in Feng et al. (2008). The security of the protocol is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP) and it achieves a good energy balance among the group members. The computation cost of the examined protocol is $2n^3 - 2n^2 + n$ scalar multiplications. Regarding its communication cost, it is $2n^2 - n$ sent messages and $2n^3 - 3n^2 + n$ received messages, whose size is 160 bits. According to our research, even if the protocol in question achieves a good energy balance, it is the most expensive constant round GKA protocol, in terms of energy consumption. This protocol is the only one with cubic computational and communication complexity. The protocol also takes consideration of join and leave operations. In particular, the computation cost of a member's join operation is $7n + 2$ scalar multiplications, while the corresponding cost for a leave operation is $5n - 10$ scalar multiplications. The communication cost will be equal to $3n + 3$ sent messages and $3n^2 + 3n$ received messages for a join operation, and $3n - 5$ sent messages and $3n^2 - 11n + 10$ received messages for a leave operation.

4.3.1.5. *Unauthenticated protocols*. In this subsection, the unauthenticated two-round protocols are presented. The first two protocols are based on the different computational capabilities of network nodes; the following protocol is based on a TTP, while the next one is based on a KGC. The five protocols that follow are based on hash functions and the last one is based on a broadcast channel.

4.3.1.5.1. *NCKW04 protocol (Nam et al., 2004a)*. According to the authors of Nam et al. (2004), the majority of the proposed GKA protocols are unsuitable for Wide Area Networks (WANs). In order to solve this problem, a novel protocol is introduced in Nam et al. (2004). The proposal provides forward secrecy and it is also provably secure against passive adversaries. This protocol is closely akin to the protocol proposed in Nam et al. (2004) and their energy cost is very similar, too. However, while protocol NCKW04 (Nam et al., 2004a) is an unauthenticated protocol, protocol NKKW04 (Nam et al., 2004b) is an authenticated one and it uses digital signatures to achieve authentication; in fact, the latter protocol consists the authenticated version of the former protocol. The NCKW04 (Nam et al., 2004a) protocol brings a computation cost of $3n - 2$ modular exponentiations and a communication cost of $2n - 1$ sent messages and $n^2 - 1$ received messages, whose size is 1024 bits. It is worth mentioning that the second round's broadcast message is very large (comprised by n single messages), bringing a significant increase in the communication cost of the examined protocol.

4.3.1.5.2. *T07b protocol (Tseng, 2007b)*. Motivated by his observation that the proposed protocol in the work of Nam et al. (2005) had inherent security weakness, Tseng (2007b) proposed a new protocol, well suited for wireless networks, comprising by multiple low-performance nodes and a powerful node. This protocol is collaborative and it is provably secure under the Diffie-Hellman assumption. The computation cost of the protocol is $3n - 2$ modular exponentiations. The communication cost of the protocol is $2(n - 1)$ sent messages and $n^2 - n$ received messages. The size of the messages is 1024 bits. Like many other GKA protocols, this protocol requires from the powerful node in the network to broadcast very large messages and this fact increases the total communication cost.

4.3.1.5.3. *ZGL10 protocol (Zhao et al., 2010)*. In Zhao et al. (2010), a fault tolerant and resistant against Denial of Service (DoS) attacks GKA protocol is proposed. The protocol is also secure against replay attacks and provides perfect forward secrecy. The execution of the protocol relies on a TTP, namely the trusted server of the system. If no faults are detected during the protocol execution, the computation cost is $3n^2 - n$ modular exponentiations. Regarding its communication cost, it is $n^2 + n$ sent messages and $n^3 - n$ received messages, whose size is 1024 bits. Note that the communication cost of this protocol is extremely high, mainly because of the large size of the first round's broadcast message.

4.3.1.5.4. *BD05 protocol (Burmester and Desmedt, 2005)*. The most cited constant round (and not only) GKA protocol is the Burmester-Desmedt or BD protocol (Burmester and Desmedt, 2005) as it is commonly called. This was the first constant round GKA protocol requiring only two rounds. The protocol firstly appeared in the proceedings of Eurocrypt 1994 (Burmester and Desmedt, 1994) and has served as the basis of many other GKA protocols. In Burmester and Desmedt (2005), the authors presented a security proof of their protocol and showed that is provably secure against passive attacks, under the Diffie-Hellman assumption. By the time it was firstly published, this was a great breakthrough in group key exchange protocols since with only two broadcasts from all group members, a secret group key could be created. For this reason, it was adopted from several scientists who tried to improve it by presenting several variants of it. The protocol's main disadvantage is that it is unauthenticated. Since BD protocol is possibly the most important constant round GKA protocol and has become the basis of many contemporary protocols, we will show how it works:

1. Each user U_i selects a random integer r_i, $1 \le r_i \le p-2$, where p is a prime number, computes $z_i = g^{r_i} \bmod p$, and sents z_i to each of the other $(n-1)$ group members (g is a generator of the finite field F_p).
2. Each U_i computes $X_i = (z_{i+1}/z_{i-1})^{r_i} \bmod p$ and sends X_i to each of the other $(n-1)$ group members.
3. After receiving X_j, $1 \le j \le n$, U_i computes the group key $K = (z_{i-1})^{nr_i} X_i^{n-1} X_{i+1}^{n-2} \ldots X_{i+(n-2)}^1 \bmod p$.

The computation cost of the BD protocol is $3n$ modular exponentiations, while its communication cost is $2n$ sent messages and $2n(n - 1)$ received messages, whose size is 1024 bits.

4.3.1.5.5. *ZR04 protocol (Zou and Ramamurthy, 2004)*. A GKA protocol based on a generalization of Diffie-Hellman protocol is proposed in Zou and Ramamurthy (2004). Similarly to the protocol in Balachandran et al. (2005), the proposal in Zou and Ramamurthy (2004) does not require member serialization, or a central trusted entity. Furthermore, Zou and Ramamurthy (2004) provides a comparison of some group Diffie-Hellman protocols. The computation cost of ZR04 (Zou and Ramamurthy, 2004) is n^2 modular exponentiations. The communication cost of the protocol is n^2 sent messages and $n^3 - n^2$ received messages. The size of each message is 1024 bits. This protocol has a quite common drawback concerning its communication cost: in the second round, every user has to broadcast a message as large as $n - 1$ different messages. The protocol also discusses the case of a mass join/leave operation. In particular, if m is the number of members that join/leave the group, then a mass join operation requires $n^2 + m^2 + 2mn - n$ exponentiations, $n^2 + m^2 + 2mn$ messages should be sent and $n^3 + m^3 - 2n^2 - m^2 + 3m^2n + 3n^2m - 2mn + n$ messages will be received. A mass leave operation will need $(n - m)(n - m - 1)$ exponentiations, $(n - m)(n - m - 1)$ messages will be sent and $(n - m)(n - m - 1)^2$ messages will be received.

4.3.1.5.6. *BRZV05 protocol (Balachandran et al., 2005)*. The authors of Balachandran et al. (2005) introduce a GKA protocol, which does not require a central entity or member serialization. These properties make it proper for mobile ad hoc networks. Moreover, the proposed protocol is fully collaborative, since it brings the same level of workload to all participants, it is computationally efficient and dynamic. For its execution, the protocol is based on the Chinese Remainder Theorem (CRT). The computation cost of this protocol is n^2 exponentiations, while its communication cost is equal to $2n$ sent messages and $2n(n - 1)$ received messages, whose size is 1024 bits. The authors also discuss the operations that should be performed when a member joins or leaves the group. In particular, a join operation requires $n-2$ exponentiations, while $n + 3$ messages are sent and $3n$-3 messages are received in total. A leave operation has a communication cost equal to 1 sent and $n-2$ received messages.

4.3.1.5.7. *T05a protocol (Tseng, 2005a)*. In Tseng (2005a), Tseng introduced an unauthenticated GKA protocol, which is robust and resistant to malicious participants. This protocol is provably secure against passive insider attacks under the Diffie-Hellman assumption in the random oracle model. Its computation cost arises to $4n^2 + n$ modular exponentiations. Its communication cost is equal to $5n$ sent messages and $5n(n-1)$ received messages, whose size is 1024 bits.

4.3.1.5.8. *JKT07 protocol (Jarecki et al., 2007)*. In Jarecki et al. (2007), an innovative GKA protocol is proposed, which is able to continue its execution, even when some of the network nodes quit, or fail to complete the protocol execution. The proposal is provably secure in the standard model under the Diffie-Hellman assumption. The unique attribute of this protocol, which lets "some players to fail during protocol execution", does not allow us to compare this protocol with the rest of the examined GKA protocols. Hence, the performance evaluation of JKT07 (Jarecki et al., 2007) is excluded from our work.

4.3.1.5.9. *KT08 protocol (Kim and Tsudik, 2008)*. The protocol presented in Kim and Tsudik (2008) is based on JKT07 protocol (Jarecki et al., 2007), making an effort to improve its efficiency and flexibility. The new protocol supports group members with different failure probabilities and can spread across any LAN/WAN combination. Protocol KT08 (Kim and Tsudik, 2008) is, likewise JKT07 (Jarecki et al., 2007), excluded from our performance analysis, since they have both the property that some group members can fail during the protocol's execution.

4.3.1.5.10. *ZW08 protocol (Zhang and Wang, 2008)*. In Zhang and Wang (2008), an improved variant of Tzeng's protocol (Tzeng, 2002) was presented. The proposed protocol reduces the computational complexity, requires fewer rounds than Tzeng's protocol and relaxes the waiting time for fault-check. The protocol in question is provably secure under the standard model and the Diffie-Hellman assumption. However, despite the fact that it uses digital signatures, it falls within the unauthenticated protocols' category, since its authors state that the protocol assumes for authentication purposes the existence of an authenticated broadcast channel (Zhang and Wang, 2008). Without this channel, the protocol has the characteristics of an unauthenticated protocol. The computation cost of this protocol is $2n^2$ modular exponentiations. Its communication cost is $n^2 + 2n$ sent messages and $n^3 + n^2 - 2n$ received messages, while the size of each message is 1024 bits. A significant drawback of this protocol, which greatly augments its communication cost, is the large size of the second round's broadcast messages.

4.3.1.6. *Authenticated and unauthenticated protocols*. In this subsection, we examine the two-round protocols, which are presented in the corresponding papers in both an authenticated and an unauthenticated version. The first pair of protocols is based on a Certification Authority; the next two are based on the different computational capabilities of network nodes, while the following pair of protocols is based on a KGC and on hash functions. Finally, the last three protocols -that come from the same paper- are based on bilinear pairings.

4.3.1.6.1. *LLC06 protocols (Lin et al., 2006)*. A GKA protocol suitable for secure teleconferencing is presented in Lin et al. (2006). The protocol comes in two variants, namely the authenticated and the unauthenticated, while both form the same group key and are based on Weil pairings. The computation cost of the unauthenticated protocol is $2n$ modular exponentiations, $2n$ pairings and $2n$ scalar multiplications. The communication cost of the unauthenticated protocol is $2n$ sent messages and $2n(n-1)$ received messages, while the size of each message is 160 bits. The computation cost of the authenticated protocol is equal to the computation cost of the corresponding unauthenticated protocol. Regarding the communication cost of the authenticated protocol, it is $3n$ sent messages and $3n(n-1)$ received messages.

4.3.1.6.2. *D07 protocol (Dutta, 2007)*. In Dutta (2007), R. Dutta has presented a password-based variant of protocol DB05 (Dutta and Barua, 2005a). The security of the protocol against dictionary attacks is proved in the ideal cipher model, under the Decisional Diffie-Hellman assumption. The author proposes a variant of the unauthenticated version of protocol DB05 (Dutta and Barua, 2005a) and based on it, she also builds the authenticated, password-based variant. The computation cost of the unauthenticated protocol is $3n$ exponentiations and its communication cost is $3n - 2$ sent messages and $n^2 + 2n - 3$ received messages. The size of each message is 1024 bits. For the completion of the authenticated protocol, apart from the abovementioned actions, the users need to execute symmetric encryption operations, which comprise the only difference between the authenticated and the unauthenticated protocol. Thus, the energy cost of both protocols is equal.

4.3.1.6.3. *LLT09 protocols (Lee et al., 2009)*. Another GKA protocol is proposed in Lee et al. (2009), presented both in its authenticated and in its unauthenticated version. This protocol is based on bilinear pairings and it is provably secure under the Diffie-Hellman assumption. In addition, this protocol is provably collaborative and uses as a basis the work of Tseng (2007b). The total computation cost brought by the unauthenticated version of the protocol is $3n - 2$ scalar multiplications and n pairings. As for its communication cost, it is $2n - 2$ sent messages and $n^2 - n$ received messages, while each message has size 160 bits. Regarding the authenticated protocol, its computation cost is $4n - 2$ scalar multiplications and $5n - 4$ pairings, while its communication cost is $3n - 2$ sent messages and $n^2 + n - 2$ received messages. Both of the abovementioned protocols display a drawback in their communication performance, which is the second round's broadcast message, sent by the powerful node of the network. In the case of the unauthenticated protocol, this message is as large as $n - 1$ separate messages, while in the case of the authenticated protocol is equal to n single messages.

4.3.1.6.4. *CHL04 protocols (Choi et al., 2004)*. In Choi et al. (2004), two GKA protocols, based on bilinear pairings are introduced. The first protocol is a bilinear variant of Burmester-Desmedt (BD) protocol (Burmester and Desmedt, 2005), while the second constitutes the ID-based authenticated version of it. The unauthenticated protocol substitutes the generators in BD protocol with pairings, while the authenticated protocol provides a mechanism of simultaneous batch verification of the received group messages, which improves the computational complexity. Both protocols provide forward secrecy and they are provably secure, under the Decisional Bilinear Diffie-Hellman assumption. The computation cost of the unauthenticated protocol is $3n$ scalar multiplications and $2n$ pairings. Its total communication cost is $2n$ sent messages and $2n(n-1)$ received messages, while the size of each message is 160 bits. The computation cost of the authenticated protocol is $8n$ scalar multiplications and $4n$ pairings. The communication cost of the latter protocol is $3n$ sent messages and $3n(n-1)$ received messages, whose size is 160 bits.

4.3.1.6.5. *DB05 protocols (Dutta and Barua, 2005a)*. In Dutta and Barua (2005a), two fully symmetric GKA protocols are presented. Both the authenticated and the unauthenticated variants of the proposed protocol are provably secure, under the Diffie-Hellman assumption. The unauthenticated protocol of Dutta and Barua (2005a) brings a computation cost equal to $3n$ modular exponentiations. The communication cost is $3n$ sent messages and n^2+n received messages, the size of which is 1024 bits. For the sake of authentication, the second protocol in Dutta and Barua (2005a) uses digital signatures; a fact which augments the energy consumption brought by the protocol's execution. The computation cost of the authenticated protocol is $2n^2+7n$ modular exponentiations, while its communication cost is $6n$ sent messages and $2n^2+2n$ received messages. The DB05 protocols also take account of mass join/leave operations. If we denote by m the number of join/leave members, then a mass join operation will cost $2m^2+19m+39$ exponentiations, $6m+22$ sent messages and $2m^2+2mn+8m+10n-6$ received messages. The corresponding cost of a mass leave operation is $2n^2+2m^2-4mn-3n+27m$ exponentiations, while $2n+6m$ messages will be sent and $2n^2+2m^2-4mn-2n+10m$ messages will be received. Finally, we would like to note that in Dutta and Barua (2008), the same authors have provided the security proof of their protocols.

4.3.1.6.6. *DL08 protocols (Desmedt and Lange, 2008)*. Two unauthenticated two-round protocols, designed with the purpose to reduce the existent computational complexity, are proposed in Desmedt and Lange (2008). The computation cost of the first of the protocols proposed in Desmedt and Lange (2008) comes to $3n/2$ modular exponentiations, n scalar multiplications and $2n$ pairings, while its communication cost is equal to $5n/2$ sent messages and $n^2/2+2n$ received messages. Regarding the second protocol proposed in Desmedt and Lange (2008), it brings a computation cost of $3n/2$ exponentiations, n scalar multiplications and $3n/2$ pairings. The communication cost of this protocol is $7n/2$ sent and $3n+n\log_4 n$ received messages. The size of each message is 160 bits, for both of the abovementioned protocols. It is worth mentioning that the authors of Desmedt and Lange (2008) recommend the execution of their second protocol, which is more efficient for a large number of protocol participants. Both unauthenticated protocols can be transformed into authenticated ones by incorporating a signature scheme. In our performance evaluation, we included the authenticated version of their second, more efficient protocol. The computation cost of this authenticated protocol comes to $3n/2$ exponentiations, $9n/2+2n\log_4 n$ scalar multiplications and $3n/2$ pairings, while its communication cost is equal to the one of its unauthenticated version.

4.4. *One-round group key agreement protocols*

In this subsection we examine ten GKA protocols, which complete their execution in only one communication round and they all are authenticated. We start with two protocols based on ID-PKI and on bilinear pairings. Next, we present four more protocols based on a KGC (2 protocols) or a TTP (2 protocols) for their execution and two more based on the different computational capabilities of network nodes. The last two protocols are extracted from the same work (Tzeng and Tzeng, 2000) and are based on hash functions.

Finally, we would like to note that a generic framework for the establishment of one-round GKA protocols, based on key encapsulation mechanisms is presented in Gorantla et al. (2009). Moreover, a one-round *asymmetric* GKA protocol is proposed in Zhang et al. (2010). In this case, the group members share a common encryption key, but they have different decryption keys.

4.4.1. *SCL05 protocol (Shi et al., 2005)*

The majority of the authenticated GKA protocols make use of digital signatures, in order to provide authentication services. However, the verification of all these signatures increases a lot the energy cost and led the authors of Shi et al. (2005) to the proposal of an authenticated protocol which does not rely on digital signatures. The protocol is based on a modified ID-based Public Key Infrastructure (ID-PKI). The proposed protocol is provably secure under the Discrete Logarithm Problem. The computation cost brought by the execution of this protocol is n^2 scalar multiplications and n pairings. Its communication cost is $n(n-1)$ sent messages and $n(n-1)$ received messages, whose size is 160 bits. A drawback of this protocol is that the messages sent by the participants are very large.

4.4.2. *HH07 protocol (He and Han, 2007)*

In He and Han (2007), a new one-round authenticated GKA protocol is presented, which is based on a modification of the ID-PKI proposed in Shi et al. (2005). This modification provides security against impersonation attacks. Although both protocols are based on the same modified ID-PKI and on the same attributes of bilinear pairings, HH07 (He and Han, 2007) requires much more computations to be executed, since it involves verification procedures. The protocol is provably secure against insider attacks, such as impersonation attacks. The computation cost of this protocol is $3n^2$ scalar multiplications and $3n$ pairings. The communication cost of the protocol is $3n(n-1)$ sent messages and $3n(n-1)$ received messages. The size of each message is 160 bits.

4.4.3. *KKHY04 protocol (Kim et al., 2004b)*

In Kim et al. (2004), an ID-based GKA protocol is proposed. This protocol relies on a trusted KGC for its execution. For authentication purposes, the protocol uses digital signatures. The total computation cost of this protocol is n^2+4n scalar multiplications and $4n^2-3n$ pairings. Regarding its communication cost, it is equal to $3n$ sent messages and $3n(n-1)$ received messages, whose size is 160 bits.

4.4.4. *XHX09 protocol (Xia et al., 2009)*

Another ID-based GKA protocol, which is executed in network level, is introduced in Xia et al. (2009). The novelty of this protocol lies in the fact that different members, from different domains can agree upon a common secret key. The IP addresses, as well as the MAC addresses of the protocol participants, serve as their public keys. Regarding the computation cost of the protocol in question, it is calculated to be $3n^2 - 2n$ scalar multiplications and $n^2 + n$ pairings, while its communication cost is $2n(n-1)$ sent and $2n(n-1)$ received messages, whose size is 160 bits.

4.4.5. *ZSM06 protocols (Zhou et al., 2006)*

According to the authors' claims, their protocol (Zhou et al., 2006) is the first one-round GKA protocol, which is secure against active attacks. The proposed protocol is based on bilinear pairings and it is provably secure in the random oracle model under the Diffie-Hellman assumption. Apart from the one-round protocol in Zhou et al. (2006), a more efficient, in communication terms, two-round protocol is proposed. The computation cost of the one-round protocol is $n(n-1)$ pairings. The communication cost of this protocol is $n(n+1)$ sent messages and $n(n+1)(n-1)$ received messages, whose size is 160 bits. Notice that although this protocol's execution completes in only one round, its communication cost is enormous, since each user needs to broadcast $n+1$ messages. Regarding the two-round protocol, its computation cost is equal to $n^2 + 2n$ scalar multiplications and $4n - 2$ pairings, while its communication cost is $3n$ sent messages and $3n^2 - n - 2$ received messages. In the case of the two-round protocol, the broadcast message of the first round remains large, but it is broadcasted only by the initiator of the protocol, which significantly reduces the communication cost of this protocol, compared to the one-round protocol.

4.4.6. *BN03 protocol (Boyd and Nieto, 2003)*

In Boyd and Nieto (2003), a provably secure GKA protocol is proposed. This protocol is more efficient than the rest of the provably secure protocols proposed until 2003 in the literature, but it does not provide perfect forward secrecy. The property of perfect forward secrecy would be impossible to be satisfied by protocol BN03 (Boyd and Nieto, 2003), since the "secured" values are only send by the initiator of the protocol. Thus, if an entity achieves to impersonate the initiator of the protocol, the session key will be forged. In addition, apart from the initiator's contribution to the session key, all others' contributions are sent in plaintext. The computation cost of the protocol in Boyd and Nieto (2003) is $4n - 3$ modular exponentiations. As for its communication cost, it is $2n - 1$ sent messages and $2n(n-1)$ received messages, whose size is 1024 bits.

4.4.7. *LLL07 protocol (Lee et al., 2007)*

In (Lee et al. (2007), a GKA protocol, designed especially for TETRA networks is proposed. Although these networks have numerous advantages, the application of conventional key agreement protocols on them brings a very high communication cost. To give a solution to the aforementioned problem, the authors of Lee et al. (2007) present an efficient protocol, well suited for TETRA networks, which provides key agreement among low-performance mobile devices and a powerful base station. The performance evaluation of this protocol is excluded from our paper, since it addresses solely to TETRA networks and it assumes that there exist Key-Encrypting Keys (KEK), before the execution of the main GKA protocol.

4.4.8. *TT00 protocols (Tzeng and Tzeng, 2000)*

Two one-round GKA protocols, secure against passive and active adversaries, are proposed in Tzeng and Tzeng (2000). The authors of Tzeng and Tzeng (2000) state that these protocols allow no leakage of useful information to passive adversaries, while they also achieve fault tolerance against any coalition of malicious system insiders. The protocols are provably secure in the random oracle model. The first one uses a system called non-interactive publicly verifiable secret (NIPVS), as well as digital signatures for authentication purposes. The second protocol of Tzeng and Tzeng (2000) uses a system called non-interactive authenticated publicly verifiable secret (NIAPVS), which eliminates the need of digital signatures. The former protocol brings a computation cost equal to $5n^2 + 2n$ modular exponentiations and a communication cost of $n(2n+3)$ sent messages and $n(2n+3)(n-1)$ received messages, which have size 1024 bits. Regarding the latter protocol, it brings a computation cost of $4n^2 + n$ modular exponentiations and it also slightly reduces the communication cost to $2n^2 + n$ sent messages and $2n^3 - n^2 - n$ received

Table 2 – Five and four-round protocols' computations having negligible cost.

Protocol	Number of Encryptions	Number of Decryptions	Number of Hash functions	Number of projective key generations	Number of master key generations
AP06 (Abdalla and Pointcheval, 2006)	–	–	$3n$ (common) $3n$ (projective) $5n$ (universal)	$3n$	n^2
JV96 (Just and Vaudenay, 1996)	–	–	$2n$	–	–
BS06 (Bohli and Steinwandt, 2006)	–	–	$n^2 + 6n$	–	–
TYO07 (Tso et al., 2007)	–	–	$n^2 + n + 1$	–	–
WRLP08 (Wan et al., 2008)	–	–	$4n$	–	–
FXW09 (Fu et al., 2009)	–	–	$2n$ (universal) n^2 (common)	–	–
Y04 (Yi, 2004)	–	–	$3n^2 - 2n + 1$	–	–
ABCP06 (Abdalla et al., 2006)	n	$2n$	$3n$	–	–
ZZLC09 (Zheng et al., 2009)	n	$2n$	$3n$	–	–

Table 3 – Complexity analysis of five and four-round protocols.

Protocol	Number of exponentiations	Number of pairings	Number of scalar multiplications	Number of sent messages	Number of received messages
AP06 (Abdalla and Pointcheval, 2006)	$2n^2 + 6n$	–	–	$11n$	$11n(n - 1)$
JV96 (Just and Vaudenay, 1996)	$4n$	–	–	$3n$	$n^2 + n$
BS06 (Bohli and Steinwandt, 2006)	$2n(n + 1)$	–	–	$7n$	$7n(n - 1)$
TYO07 (Tso et al., 2007)	$2n^2 + 5n$	–	–	$n^2 + 5n + 1$	$4n^2 + n$
WRLP08 (Wan et al., 2008)	–	$2n$	$n^2 + 5n - 3$	$9n - 7$	$2n^2 + 5n - 7$
FXW09 (Fu et al., 2009)	$7n$	–	–	$5n$	$2n^2 + n$
Y04 (Yi, 2004)	$2n$	$2n^2$	$7n$	$n^2 + 3n + 1$	$3n^2 + 2n$
ABCP06 (Abdalla et al., 2006)	$3n$	–	–	$4n$	$4n(n - 1)$
ZZLC09 (Zheng et al., 2009)	$5n$	–	–	$4n$	$4n(n - 1)$

messages. Both of the aforementioned protocols display a significant drawback in their communication cost; the first one requires its participants to broadcast a set of $2n + 3$ messages, while the second one requires its participants to broadcast a set of $2n + 1$ messages, each, which in both cases augments greatly the protocols' communication cost.

5. Performance evaluation

In this Section, we summarize the computation and communication cost of all protocols in appropriate tables and we present their energy cost in corresponding figures, using various group sizes. Each subsection includes the performance evaluation of the corresponding protocols presented in Section 4, while there are two additional subsections presenting the five most efficient authenticated and unauthenticated protocols, respectively. In order to be more precise on the way we computed the total energy cost for each protocol, we present an example. Suppose that we wish to compute the total energy cost of ABCP06 protocol (Abdalla et al., 2006) for various group sizes $n = 125, 216, 343, 512, 729$ and 1000. The operations mentioned in Table 2 have negligible cost and therefore we take into account only the amounts mentioned in Table 3. Then, using also Table 1, we compute that the computation cost of ABCP06 protocol (Abdalla et al., 2006) is equal to $3n \times 9.1$ mJ $= 27.3n$ mJ while the communication cost is $4n \times 0.66$ μJ $\times 1024 + 4n(n - 1) \times 0.31$ μJ $\times 1024 = 2.7n$ mJ $+ 1.27n(n - 1)$ mJ. We multiplied with 1024 since the size of a single message for this protocol is 1024 bits.

5.1. *Performance evaluation of Section 4.1 protocols*

Table 2 summarizes the computations taking place during the execution of the five and four-round protocols, which have negligible energy cost. Thus, these computations do not affect the final performance evaluation and the assessment of the protocols' total energy cost. In Table 3, we summarized the total computation and communication cost of the five and four-round GKA protocols. These actions have impact in the total energy consumption of each protocol and are used for the construction of the comparative graphs that follow.

In order to compare the protocols properly, we divided the examined protocols into two categories: the most efficient and the least efficient protocols. From Fig. 1, it is obvious that protocol Y04 (Yi, 2004) has a computation cost, which is much higher than the average of the other protocols. On the other side, protocol WRLP08 (Wan et al., 2008) is the most efficient, in terms of computation, from the protocols depicted in Fig. 1. Protocols AP06 (Abdalla and Pointcheval, 2006), TYO07 (Tso et al., 2007) and BS06 (Bohli and Steinwandt, 2006) have similar computation cost, which is also obvious from their complexity analysis in Table 3. In Fig. 2, we present the most efficient five and four-round protocols, in terms of computation cost. Protocol ABCP06 (Abdalla et al., 2006) has the smallest computation cost, followed by JV96 (Just and Vaudenay, 1996), ZZLC09 (Zheng et al., 2009) and FXW09 (Fu

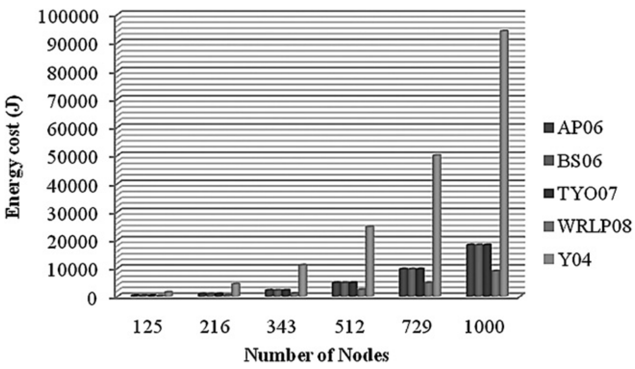

Fig. 1 – Computation cost of the least efficient five and four-round protocols.

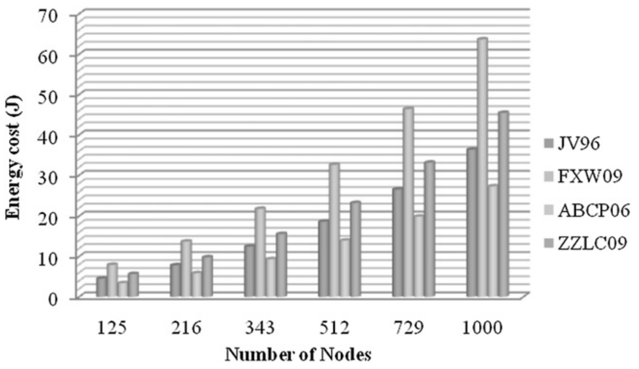

Fig. 2 – Computation cost of the most efficient five and four-round protocols.

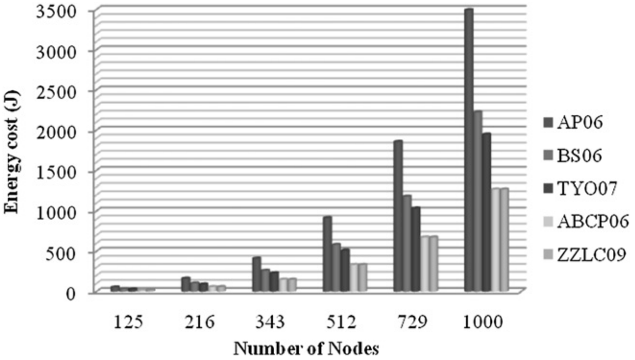

Fig. 3 – Communication cost of the least efficient five and four-round protocols.

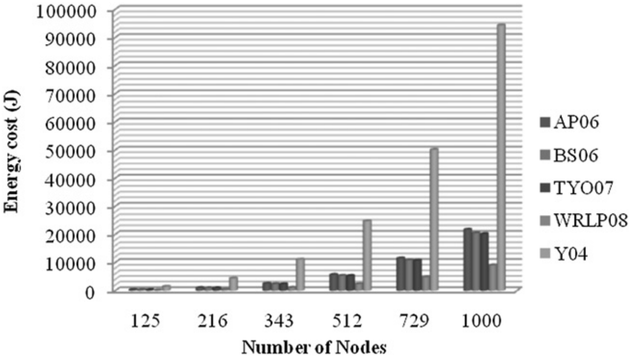

Fig. 5 – Total energy cost of the least efficient five and four-round protocols.

et al., 2009). Notice that all these protocols have linear computational complexity.

Regarding the communication cost of the protocols, we notice that the only protocols with square complexity of sent and received messages are TYO07 (Tso et al., 2007) and Y04 (Yi, 2004), while the rest of the examined protocols display linear complexity of sent messages and square complexity of received messages. However, as depicted in Fig. 3, AP06 (Abdalla and Pointcheval, 2006) and BS06 (Bohli and Steinwandt, 2006) have the largest communication cost, with the former protocol displaying the worst performance. Notice that the communication cost of protocol Y04 (Yi, 2004) is significantly reduced by the small size of the exchanged messages, which is equal to 160 bits only. Protocol TYO07 (Tso et al., 2007) comes next, with a relatively high communication cost. An also high, but lower than the one of TYO07 (Tso et al., 2007), communication cost is brought by protocols ABCP06 (Abdalla et al., 2006) and ZZLC09 (Zheng et al., 2009), which have exactly the same communication cost.

The remaining protocols, which display a much better performance regarding their communication cost, are depicted in Fig. 4. It is easy to see that protocol FXW09 (Fu et al., 2009) brings the highest communication cost of those four protocols. Protocol JV96 (Just and Vaudenay, 1996) comes next, with a relatively low communication cost, even if it is the oldest constant round GKA protocol proposed in the literature. It is interesting that Y04 protocol (Yi, 2004) is quite efficient, even though it has square complexity of sent messages. Clearly, the communication efficiency is affected not only by the total number of exchanged messages, but also by their size (which is equal to only 160 bits for Y04 protocol (Yi, 2004)). Finally, WRLP08 (Wan et al., 2008) is the most efficient, in terms of communication, of all of the five and four-round protocols. In Fig. 5, we can observe that protocol Y04 (Yi, 2004) displays the worst performance in overall, with a relatively big cost difference from the rest of the examined protocols. This comes, mainly, as a result of this protocol's high computation cost. The protocols that follow are AP06 (Abdalla and Pointcheval, 2006) and BS06 (Bohli and Steinwandt, 2006), with slight energy cost differences between them, followed by protocol TYO07 (Tso et al., 2007), which owes its relatively high cost, to its high communication complexity. Finally, a medium performance is displayed by protocol WRLP08 (Wan et al., 2008). According to Fig. 6, the most efficient protocol in this category is JV96 (Just and Vaudenay, 1996), followed by protocol FXW09 (Fu et al., 2009). ZZLC09 (Zheng et al., 2009) and ABCP06 (Abdalla et al., 2006) protocols are also quite efficient and have similar total energy cost.

5.2. *Performance evaluation of Section 4.2 protocols*

In this subsection we examine the performance of the three-round GKA protocols. The computations taking place during

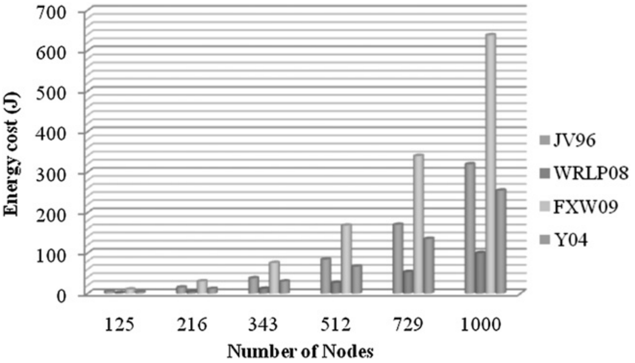

Fig. 4 – Communication cost of the most efficient five and four-round protocols.

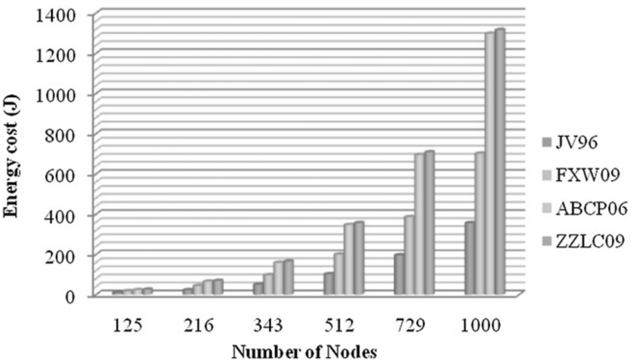

Fig. 6 – Total energy cost of the most efficient five and four-round protocols.

Table 4 – Three-round protocols' computations having negligible cost.

Protocol	Number of Hash functions
NKYW04 (Nam et al., 2004c)	$2n + m$
YWJ08 (Yao et al., 2008)	$2n^2 + 2n$
YHVK08 (1) (Yeun et al., 2008)	n^2
YHVK08 (2) (Yeun et al., 2008)	$2n^2 + 5n$
BC04a (Bresson and Catalano, 2004a)	$2n$
NLKW05 (Nam et al., 2005)	n
ABIS07 (Augot et al., 2007)	–
HLL07 (Hu et al., 2007)	$3n - 2$

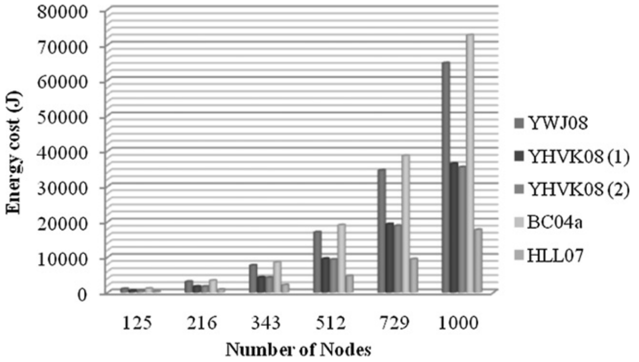

Fig. 7 – Computation cost of the least efficient three-round protocols.

each protocol's execution and require negligible energy consumption are presented in Table 4. Note that by YHVK08 (1) we denote the enhanced Burmester-Desmedt protocol, while by YHVK08 (2), we denote the enhanced Choi et al. protocol, which were both presented in Yeun et al. (2008). Table 5 summarizes the energy consuming operations that are executed in each GKA protocol. The examined protocols are divided into two categories: the least efficient and the most efficient protocols. This is necessary for the proper comparison of the protocols in the figures that follow.

In Fig. 7, we see the computation cost of the three-round protocols with the worst performance. BC04a (Bresson and Catalano, 2004a) is the most energy consuming, followed closely by YWJ08 (Yao et al., 2008). A high computation cost is displayed also by protocols YHVK08 (1) and YHVK08 (2) (Yeun et al., 2008). Finally, among these protocols (notice that all have square computation cost), the most efficient is HLL07 (Hu et al., 2007), requiring much less energy for computations than the abovementioned protocols. The computation cost of the rest of the three-round protocols is presented in Fig. 8. As it is obvious from Fig. 8, these protocols have a much smaller computation cost than the abovementioned protocols. This comes as a result of their linear computational complexity. From these protocols, the highest cost is brought by NPKW07 (Nam et al., 2007), NKYW04 (Nam et al., 2004c) and PHYK08 (Park et al., 2008). The most efficient protocol, in computation terms, is NLKW05 (Nam et al., 2005), followed closely by ABIS07 (Augot et al., 2007).

In Fig. 9, we present the communication cost of the least efficient three-round protocols. We notice that BC04a protocol (Bresson and Catalano, 2004a) is not only the most consuming protocol in terms of computation but also has the highest communication cost of all three-round protocols. The reason for this large energy consumption is its square complexity of sent and received messages. YHVK08 (1) protocol (Yeun et al., 2008) has also a high communication cost. Protocols ABIS07 (Augot et al., 2007) and NLKW05 (Nam et al., 2005) have similar communication costs with NLKW05 protocol having the best performance among the protocols in this group. The most efficient protocols concerning the communication cost are presented in Fig. 10. Protocols YHVK08 (2) (Yeun et al., 2008), YWJ08 (Yao et al., 2008) and HLL07 (Hu et al., 2007) have similar communication cost, while PHYK08 (Park et al., 2008), NKYW04 (Nam et al., 2004c) and NPKW07 (Nam et al., 2007) are the most efficient of the three-round GKA protocols (in terms of communication).

In Fig. 11, we see the total energy cost brought by the least efficient three-round GKA protocols. The worst performance is demonstrated by BC04a protocol (Bresson and Catalano, 2004a). The total energy cost of YWJ08 protocol (Yao et al., 2008) is also high, mainly due to its huge computation cost. Protocols YHVK08 (1) (Yeun et al., 2008) and YHVK08 (2) (Yeun et al., 2008) have similar energy costs, while HLL07 (Hu et al., 2007) is much more efficient than the previously mentioned protocols. In Fig. 12, we show the energy cost of the five most efficient three-round protocols. The least efficient protocol

Table 5 – Complexity analysis of three-round protocols.

Protocol	Number of exponentiations	Number of pairings	Number of scalar multiplications	Number of sent messages	Number of received messages
NKYW04 (Nam et al., 2004c)	$mn - m^2 + 2m + 3n + 1$	–	–	$n + 2m + 1$	$3\ nm + 3n - m - 3$
PHYK08 (Park et al., 2008)	–	$2n + 2$	$9n$	$4n$	$n^2 + 2n$
YWJ08 (Yao et al., 2008)	–	$2n^2 + 4n$	$n^2 + 5n$	$5n$	$5n(n - 1)$
YHVK08 (1) (Yeun et al., 2008)	$4n^2 + 6n$	–	–	$6n$	$6n(n - 1)$
YHVK08 (2) (Yeun et al., 2008)	–	$4n$	$4n^2 + 6n$	$6n$	$6n(n - 1)$
BC04a (Bresson and Catalano, 2004a)	$8n^2 - 3n$	–	–	$5n^2 - 3n$	$7n(n - 1)$
NLKW05 (Nam et al., 2005)	$8n - 4$	–	–	$4n - 1$	$2n^2 + n - 3$
ABIS07 (Augot et al., 2007)	$10n - 8$	–	–	$6n$	$3n^2$
HLL07 (Hu et al., 2007)	–	$2(n - 1)$	$2n^2 + 6n -4$	$4n + 2$	$4n^2 - 4$
NPKW07 (Nam et al., 2007)	$5n + n/2 + 5n \log n - 1$	–	–	$5n -2$	$2n + 10n \log n - 2$

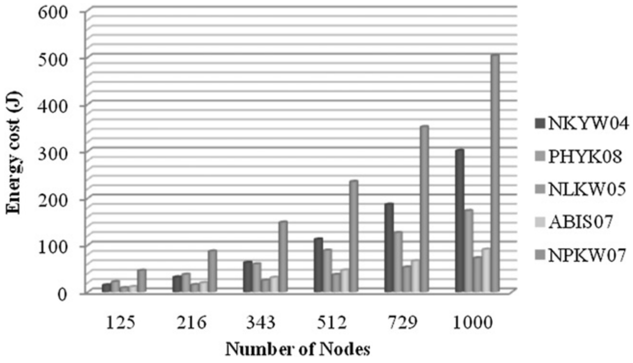

Fig. 8 – Computation cost of the most efficient three-round protocols.

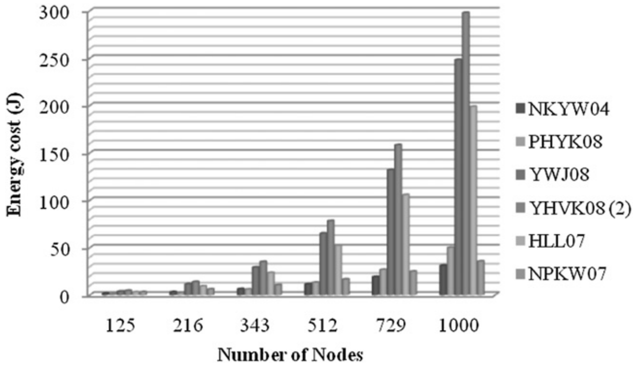

Fig. 10 – Communication cost of the most efficient three-round protocols.

among them is ABIS07 protocol (Augot et al., 2007), while the most efficient three-round protocol is PHYK08 (Park et al., 2008), followed closely by NKYW04 (Nam et al., 2004c).

5.3. *Performance evaluation of Section 4.3.1 protocols*

In this subsection, we thoroughly examine the performance of Section's 4.3.1 protocols, which are two-round authenticated protocols based on a Certification Authority or other trusted parties. In Table 6 we summarize the computations with negligible cost for these protocols, while in Table 7 we present their computational and communication complexity.

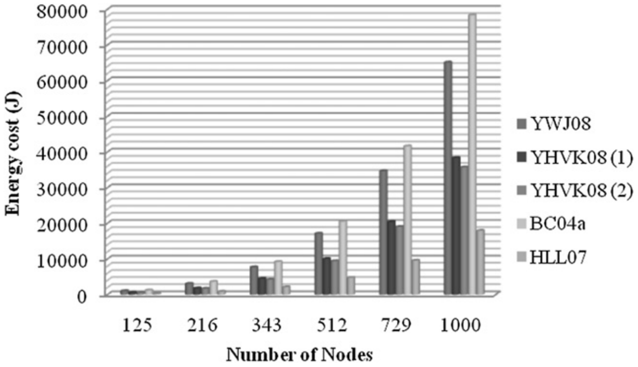

Fig. 11 – Total energy cost of the least efficient three-round protocols.

Fig. 13 shows that T05b (Tseng, 2005b) has the largest computation cost among all protocols in this category, followed by T07a protocol (Tseng, 2007a). A relatively smaller computation cost is brought by protocols ZWZ07 (Zheng et al., 2007) and ZWZL09 (Zhang et al., 2009). ZTR06 protocol (Zou et al., 2006) is the most efficient of the examined protocols in terms of computation. The computation cost of the examined protocols does not vary much, due to the fact that all of the abovementioned protocols display square computational complexity. In Fig. 14, the communication cost of the abovementioned protocols is shown. It is clear that the communication cost brought by protocols ZWZ07 (Zheng et al., 2007) and T05b (Tseng, 2005b) is extremely high, making these two protocols inexpedient. This is mainly a result of these protocols' cubic complexity of received messages and square complexity of sent messages. The rest of this category's protocols are presented in Fig. 15. These protocols have square complexity of received messages and linear complexity of sent messages. Consequently, they cannot be compared directly with protocols ZWZ07 (Zheng et al., 2007) and T05b (Tseng, 2005b). As it is obvious from Fig. 15, ZWZL09 (Zhang et al., 2009) and ZTR06 (Zou et al., 2006) are the most

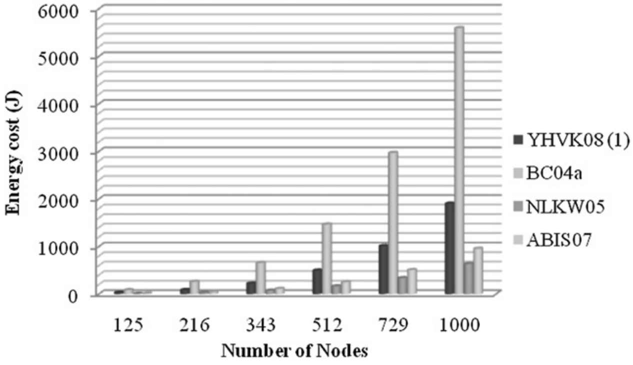

Fig. 9 – Communication cost of the least efficient three-round protocols.

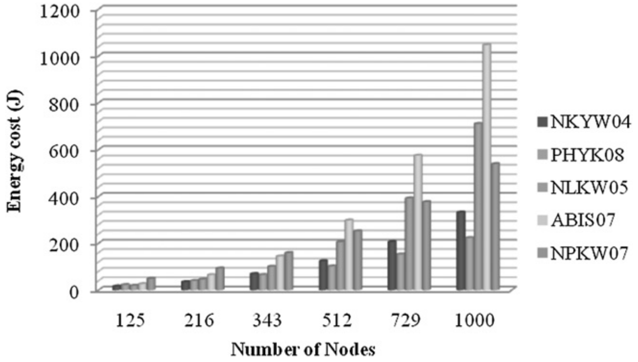

Fig. 12 – Total energy cost of the most efficient three-round protocols.

Table 6 – Computations having negligible cost for two-round authenticated protocols based on a CA or TTP.

Protocol	Number of Hash functions	Number of Greatest Common Divisor computations
T05b (Tseng, 2005b)	$2n^2$	–
T07a (Tseng, 2007a)	$2n^2$	–
ZWZ07 (Zheng et al., 2007)	n^2	N
ZTR06 (Zou et al., 2006)	$2n^2 - n$	N

efficient protocols having an equal communication cost. Because of their extremely large communication cost, ZWZ07 (Zheng et al., 2007) and T05b (Tseng, 2005b) protocols have also large total energy cost as it can be seen in Fig. 16. T07a (Tseng, 2007a) and ZWZL09 (Zhang et al., 2009) protocols have quite good performance, while the most efficient protocol of this category is ZTR06 (Zou et al., 2006).

5.4. *Performance evaluation of Section 4.3.1.2 protocols*

In this subsection we evaluate the performance of the authenticated two-round GKA protocols which are based on bilinear pairings for their execution. The following Table 8 summarizes the computations taking place during each protocol's execution and have negligible energy cost. For the rest of this section, we are going to divide the examined protocols into two categories: the least efficient and the most efficient protocols, in order to be able to discern the cost differences among them. In Table 9 we present the computation and communication cost of the protocols in question. Using this table, we have derived the figures that follow.

As it is obvious from Fig. 17, HLH07 protocol (He et al., 2007) has the highest computation cost. As it has been already mentioned, the computation of a pairing is the most energy consuming operation. This fact in combination with the square complexity of pairings and scalar multiplications of HLH07 protocol (He et al., 2007) is the reason for its high computation cost. The protocols which come next, with also high computation cost are LTL08 (Li et al., 2008) and GZG09 (Geng et al., 2009). ZSM06 (2) (Zhou et al., 2006) protocol has the lowest computation cost among all protocols in this subgroup. The computation cost of the remainder two-round pairing-based protocols is depicted in Fig. 18. The most efficient protocol, in terms of computation, is LJY05 (Li et al., 2005). TZZ08 (Tang et al., 2008) and KNKW05 (Kim et al., 2005) follow with an almost identical computation cost.

Table 7 – Complexity analysis of two-round authenticated protocols based on a CA or TTP.

Protocol	Number of exponentiations	Number of sent messages	Number of received messages
T05b (Tseng, 2005b)	$9n^2 - 5n$	$n^2 + 5n$	$n^3 + 4n^2 - 5n$
T07a (Tseng, 2007a)	$8n^2 - 2n$	$8n$	$8n(n - 1)$
ZWZ07 (Zheng et al., 2007)	$2n^2 + 3n$	$n^2 + 5n$	$n^3 + 4n^2 - 5n$
ZWZL09 (Zhang et al., 2009)	$4n^2 - n$	$6n$	$6n(n - 1)$
ZTR06 (Zou et al., 2006)	$n^2 + 3n$	$6n$	$6n(n - 1)$

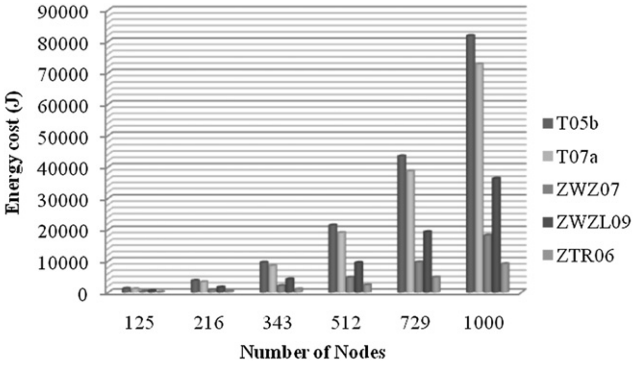

Fig. 13 – Computation cost of authenticated two-round protocols based on a CA or TTP.

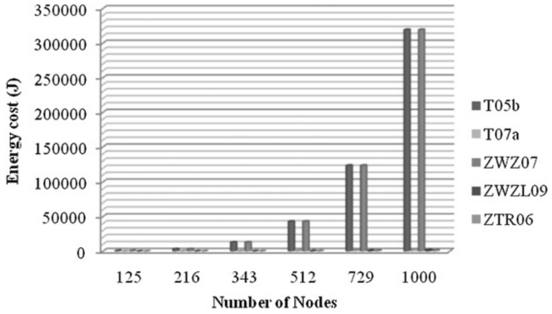

Fig. 14 – Communication cost of authenticated two-round protocols based on a CA or TTP.

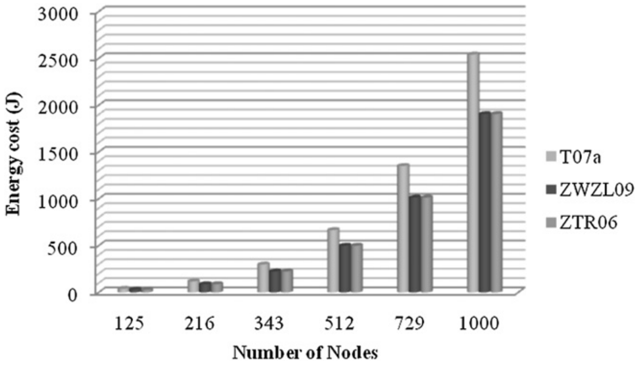

Fig. 15 – Communication cost of the efficient authenticated two-round protocols based on a CA or TTP.

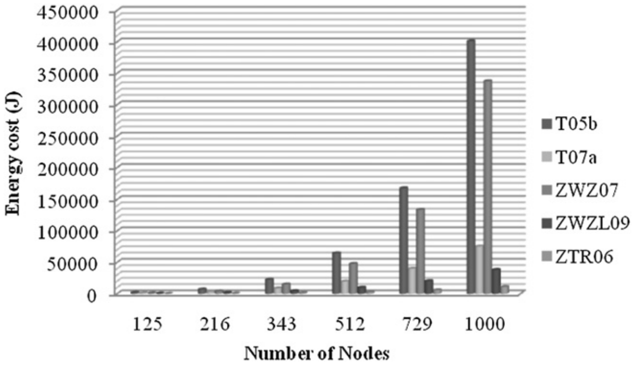

Fig. 16 – Total energy cost of authenticated two-round protocols based on a CA or TTP.

Table 8 – Computations having negligible cost of two-round authenticated protocols based on bilinear pairings.

Protocol	Number of hash functions
DWGW03b (Du et al., 2003b)	n^2
LJY05 (Li et al., 2005)	5n
KNKW05 (Kim et al., 2005)	$3(n-1)$
ZSM06 (2) (Zhou et al., 2006)	n^2+5n-2
CSCW07 (Cho et al., 2007)	$6n-4$
HLH07 (He et al., 2007)	n^2+n
CHL08 (Choi et al., 2008)	n^2+4n
CM08 (Cao and Ma, 2008)	n^2+n
LTL08 (Li et al., 2008)	$2n(n-1)$
GZG09 (Geng et al., 2009)	$4n^2-3n$
PAK09 (Park et al., 2009)	$4n-2$
LL10 (Lv and Li, 2010)	$9n$

The communication cost of the protocols in question is depicted in Figs. 19 and 20. From these figures, we have excluded protocol CM08 (Cao and Ma, 2008), due to its enormous communication cost which is by far larger than the cost of the other protocols. This really high communication cost comes as a result of the protocol's cubic complexity of received messages. Regarding the least efficient protocols, in terms of communication, it can be seen in Fig. 19 that the most energy consuming protocol is GZG09 protocol (Geng et al., 2009). An also high communication cost is brought by the execution of protocols LTL08 (Li et al., 2008) and CHL08 (Choi et al., 2008), in a descending cost order. The remainder protocols in Fig. 19 have slight differences among their costs. In Fig. 20, the communication cost of the most efficient two-round pairing-based protocols is presented. All these protocols are very efficient in terms of communication, while their costs are almost equal. However, the highest communication cost is displayed by protocol TZZ08 (Tang et al., 2008), followed by KNKW05 (Kim et al., 2005), while CSCW07 (Cho et al., 2007) comes third.

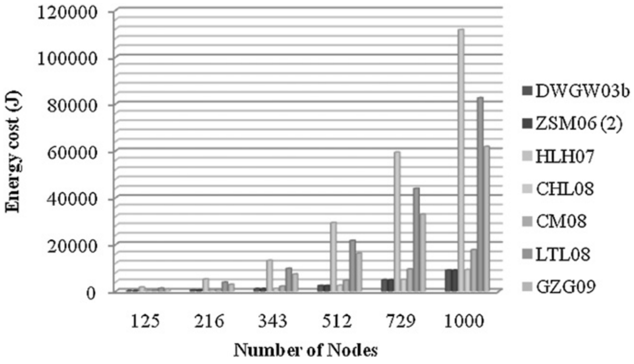

Fig. 17 – Computation cost of the least efficient two-round authenticated protocols based on bilinear pairings.

The total energy cost of the protocols in question is depicted in Figs. 21 and 22. As it is obvious from Fig. 21, the most energy consuming protocol is HLH07 (He et al., 2007) (a result of the protocol's very high computation cost). The second highest total energy cost is brought by protocol LTL08 (Li et al., 2008). CM08 protocol (Cao and Ma, 2008) has also a large total energy cost, due to its huge communication cost. The protocol that follows is GZG09 (Geng et al., 2009), while protocols DWGW03b (Du et al., 2003b), ZSM06 (2) (Zhou et al., 2006) and CHL08 (Choi et al., 2008) have slight differences

Table 9 – Complexity Analysis of two-round authenticated protocols based on bilinear pairings.

Protocol	Number of exponentiations	Number of pairings	Number of scalar multiplications	Number of sent messages	Number of received messages
DWGW03b (Du et al., 2003b)	–	4n	n^2+5n	$3n$	$3n(n-1)$
LJY05 (Li et al., 2005)	–	–	$7n$	$9n$	$3n^2+3n$
KNKW05 (Kim et al., 2005)	$n-1$	$3n-2$	$4n-1$	$3n-1$	n^2+2n-3
ZSM06 (2) (Zhou et al., 2006)	–	$4n-2$	n^2+2n	$3n$	$3n^2-n-2$
CSCW07 (Cho et al., 2007)	$3(n-1)$	$5n-4$	$4n$	$4n-1$	n^2+4n-5
HLH07 (He et al., 2007)	–	$2n^2$	$2n^2+3n$	$3n$	$3n(n-1)$
TZZ08 (Tang et al., 2008)	–	$3n$	$5n$	$3n$	n^2+n
CHL08 (Choi et al., 2008)	–	$6n$	n^2+10n	$5n$	$5n(n-1)$
CM08 (Cao and Ma, 2008)	–	$2n$	$2n^2+2n$	n^2+n	n^3-n
LTL08 (Li et al., 2008)	n^2	n^2+n	$3n^2-n$	$2n(n-1)$	$2n(n-1)$
GZG09 (Geng et al., 2009)	–	$4n$	$7n^2-5n$	$3n^2-2n$	$4n(n-1)$
PAK09 (Park et al., 2009)	–	$4n-2$	$6n$	$3n$	$3n^2-n-2$
LL10 (Lv and Li, 2010)	–	$5n$	$10n$	$3n$	$3n(n-1)$

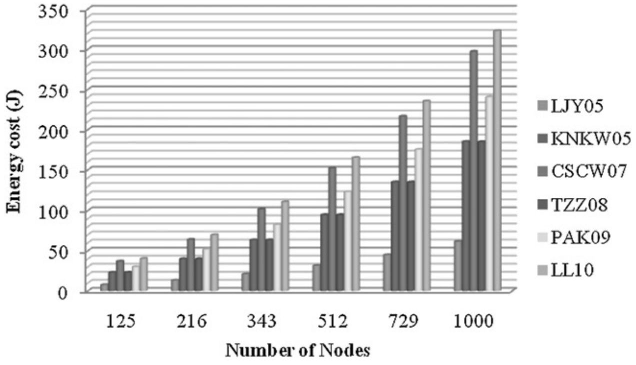

Fig. 18 – Computation cost of the most efficient two-round authenticated protocols based on bilinear pairings.

among their total energy costs. In Fig. 22, we observe that protocols LL10 (Lv and Li, 2010), PAK09 (Park et al., 2009) and CSCW07 (Cho et al., 2007), in a descending cost order, display a medium performance, in comparison with all of this category's protocols. Much more efficient are protocols TZZ08 (Tang et al., 2008) and KNKW05 (Kim et al., 2005), while protocol LJY05 (Li et al., 2005) is the most efficient protocol of all two-round pairing-based GKA protocols and owes its good performance, mainly, to its low computational complexity.

5.5. *Performance evaluation of Section 4.3.1.3 protocols*

In this subsection we evaluate the performance of the authenticated two-round GKA protocols that are based on the different computational capabilities of the network nodes. In Table 10, we present the number of required hash functions during the execution of each protocol, which bring a negligible energy cost. In Table 11 we summarize the computation and communication cost of the examined protocols. Re The total computation cost of these protocols is presented in Fig. 23. We observe that LWH09 protocol (Lu et al., 2009) has the highest computation cost, followed by CNKW05 (Cho et al., 2005) and NKKW04 (Nam et al., 2004b), with the latter protocol being slightly more efficient than the former. The computation cost of the two remaining protocols is lower with T07c protocol (Tseng, 2007c) having the best performance. It is worth mentioning, that all of this category's protocols are very efficient, in terms of computation, since they all have linear computational complexity.

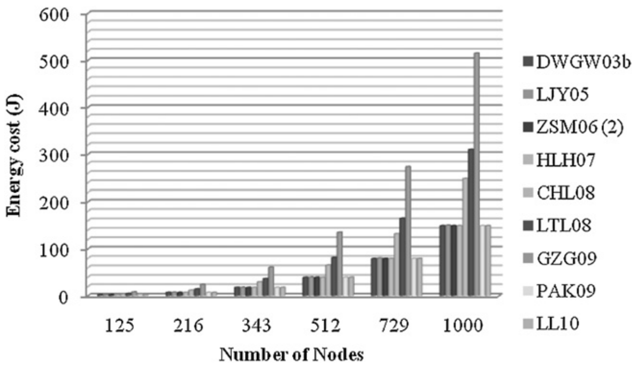

Fig. 19 – Communication cost of the least efficient two-round authenticated protocols based on bilinear pairings.

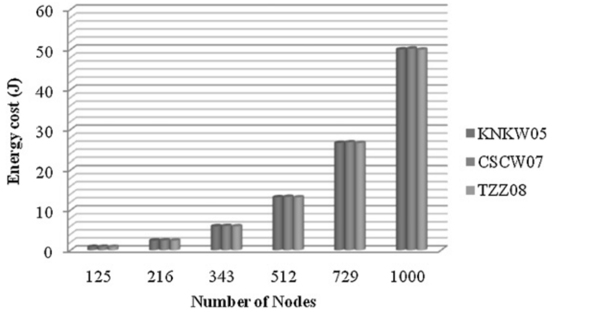

Fig. 20 – Communication cost of the most efficient two-round authenticated protocols based on bilinear pairings.

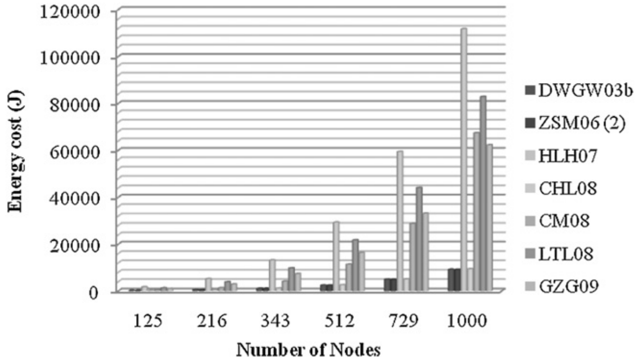

Fig. 21 – Total energy cost of the least efficient two-round authenticated protocols based on bilinear pairings.

The communication cost of the abovementioned two-round authenticated GKA protocols is depicted in Fig. 24. Protocols T07c (Tseng, 2007c) and NKKW04 (Nam et al., 2004b) have the largest communication cost, being almost equal for both protocols. CNKW05 (Cho et al., 2005) and SC09 (Saha and Chowdhury, 2009a) require much less energy, while LWH09 protocol (Lu et al., 2009) has the best performance among all examined protocols. Fig. 25 presents the total energy cost of all

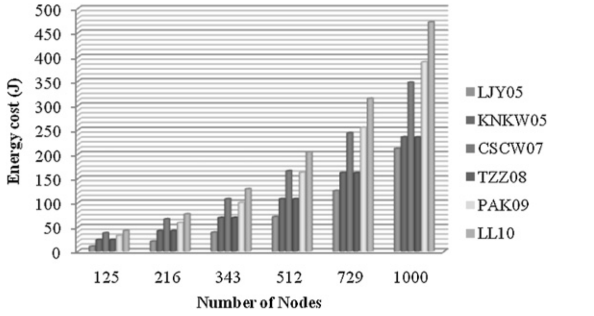

Fig. 22 – Total energy cost of the most efficient two-round authenticated protocols based on bilinear pairings.

Table 10 – Computations having negligible cost for two-round authenticated protocols based on the different computational capabilities of network nodes.

Protocol	Number of hash functions
NKKW04 (Nam et al., 2004b)	n
CNKW05 (Cho et al., 2005)	$3n - 1$
T07c (Tseng, 2007c)	n
LWH09 (Lu et al., 2009)	$8n$
SC09 (Saha and Chowdhury, 2009a)	$3n - 2$

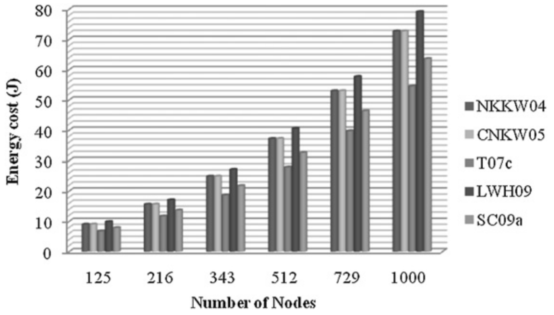

Fig. 23 – Computation cost of two-round authenticated protocols based on the different computational capabilities of network nodes.

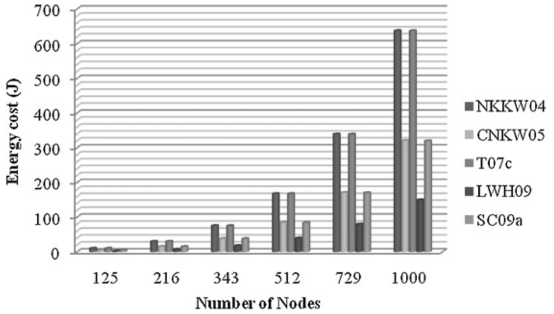

Fig. 24 – Communication cost of two-round authenticated protocols based on the different computational capabilities of network nodes.

protocols and is very similar to Fig. 24. The reason is the small computation cost of all examined protocols.

5.6. *Performance evaluation of Section 4.3.1.4 protocols*

In this subsection we examine the performance of two-round authenticated GKA protocols based on hash functions. In Table 12, we present the operations taking place during these protocols' execution and have negligible computation cost. The computation and communication cost of the examined protocols is presented in Table 13.

In Fig. 26, we present the computation cost of four of the examined protocols. Protocols FWM08 (Feng et al., 2008) and KLL04 (Kim et al., 2004a) were excluded, due to their cubic and square computational complexity, respectively. The remaining four protocols have linear computational complexity and their cost is depicted in Fig. 26. LHL04 (Lee et al., 2004) and DB06 protocols (Dutta and Barua, 2006) are the most efficient computationally, having exactly the same cost, while KJL06 (Kwon et al., 2006) and TT05 (Tan and Teo, 2005) follow. In Fig. 27, the communication cost of the examined protocols, with the exclusion of protocol FWM08 (Feng et al., 2008), is depicted. This protocol was excluded due to its huge communication cost, which comes as a result of its square complexity of sent messages and cubic complexity of received messages. Concerning the cost of the remaining protocols, the highest communication cost is brought by protocols TT05 (Tan and Teo, 2005) and KLL04 (Kim et al., 2004a), which have exactly the same cost. Also KJL06 (Kwon et al., 2006) and LHL04 protocols (Lee et al., 2004) have exactly the same communicational performance, while DB06 (Dutta and Barua, 2006) is the most efficient protocol of this category, in terms of communication.

In Fig. 28, the total energy cost of the protocols in question is presented and the huge communication and computation cost of protocol FWM08 (Feng et al., 2008) was the reason for its exclusion from the graph. KLL04 protocol (Kim et al., 2004a) is also energy consuming due to its very high computation cost. The remaining four protocols are very efficient, with DB06 protocol (Dutta and Barua, 2006) having the best performance.

5.7. *Performance evaluation of Section 4.3.1.5 protocols*

In this subsection, we evaluate the performance of the two-round unauthenticated GKA protocols. The computations required in these protocols, having negligible cost, are summarized in Table 14. Table 14 does not include all of this

Table 11 – Complexity analysis of two-round authenticated protocols based on the different computational capabilities of network nodes.

Protocol	Number of exponentiations	Number of scalar multiplications	Number of sent messages	Number of received messages
NKKW04 (Nam et al., 2004b)	$8n - 6$	–	$4n - 2$	$2n^2 - 2$
CNKW05 (Cho et al., 2005)	$8n - 5$	–	$3n$	$n^2 + 3n - 4$
T07c (Tseng, 2007c)	$6n - 4$	–	$4n - 3$	$2n^2 - n - 1$
LWH09 (Lu et al., 2009)	–	$9n + 1$	$7n + 3$	$3n^2 + 7n - 6$
SC09 (Saha and Chowdhury, 2009a)	$7n - 6$	–	$3n - 2$	$n^2 + n - 2$

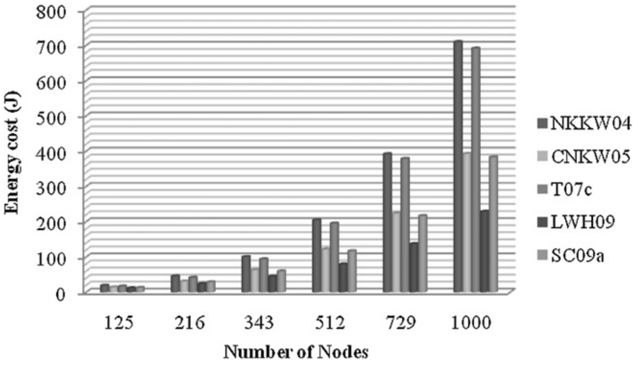

Fig. 25 – Total energy cost of two-round authenticated protocols based on the different computational capabilities of network nodes.

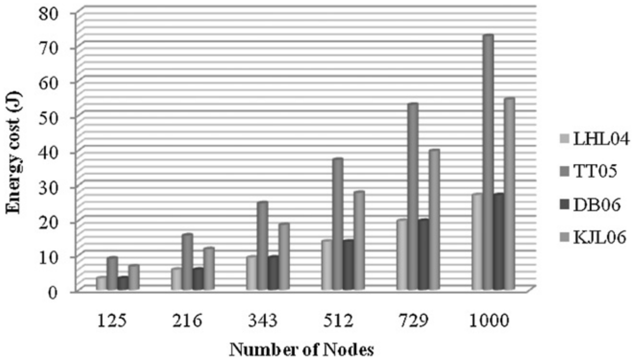

Fig. 26 – Computation cost of two-round authenticated protocols based on hash functions.

category's protocols, since some of them do not require the execution of such computations. To the contrary, Table 15 includes all of the examined two-round unauthenticated GKA protocols and assesses their computation and communication cost. For the rest of this subsection, we have divided the examined protocols into two categories: the least efficient and the most efficient protocols.

In Fig. 29, the computation cost of the least efficient two-round unauthenticated protocols is depicted. BRZV05 (Balachandran et al., 2005) and ZR04 (Zou and Ramamurthy, 2004) protocols have equal computational complexity, while the highest computation cost is brought by protocols ZGL10 (Zhao et al., 2010), ZW08 (Zhang and Wang, 2008) and T05a (Tseng, 2005a), with the latter having the worst performance. As we can observe in Fig. 30, protocols T07b (Tseng, 2007b), NCKW04 (Nam et al., 2004a) and BD05 (Burmester and Desmedt, 2005) are the most efficient, in terms of computation, from all of this category's protocols, having an obvious difference from the other five protocols. These protocols have almost the same computation cost and their good performance comes due to their linear computational complexity.

In Fig. 31, we see that the three most expensive unauthenticated protocols in terms of communication are ZW08 (Zhang and Wang, 2008), ZR04 (Zou and Ramamurthy, 2004) and ZGL10 (Zhao et al., 2010). Their large communication cost is a result of their square complexity of sent messages and cubic complexity of received messages. The communication cost of the rest of the examined protocols is presented in Fig. 32. These protocols have linear complexity of sent messages and square complexity of received messages. Among them, T05a protocol (Tseng, 2005a) has the highest

Table 12 – Computations having negligible cost of two-round authenticated protocols based on hash functions.

Protocol	Number of Encryptions	Number of Decryptions	Number of Hash functions	Number of Pseudorandom functions
KLL04 (Kim et al., 2004a)	–	–	$5n-1$	–
LHL04 (Lee et al., 2004)	n	$2n$	$3n$	–
TT05 (Tan and Teo, 2005)	–	–	$5n$	–
DB06 (Dutta and Barua, 2006)	$2n$	n^2+n	$3n$	–
KJL06 (Kwon et al., 2006)	–	–	$3n$	n
FWM08 (Feng et al., 2008)	–	–	$2n$	–

Table 13 – Complexity Analysis of two-round authenticated protocols based on hash functions.

Protocol	Number of exponentiations	Number of scalar multiplications	Number of sent messages	Number of received messages
KLL04 (Kim et al., 2004a)	$4n^2+n$	–	$5n$	$5n(n-1)$
LHL04 (Lee et al., 2004)	$3n$	–	$2n$	$2n(n-1)$
TT05 (Tan and Teo, 2005)	$8n$	–	$5n$	$5n(n-1)$
DB06 (Dutta and Barua, 2006)	$3n$	–	$3n$	n^2+n
KJL06 (Kwon et al., 2006)	$6n$	–	$2n$	$2n(n-1)$
FWM08 (Feng et al., 2008)	–	$2n^3-2n^2+n$	$2n^2-n$	$2n^3-3n^2+n$

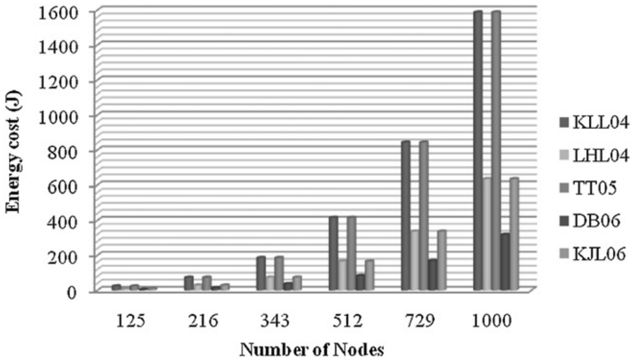

Fig. 27 – Communication cost of two-round authenticated protocols based on hash functions.

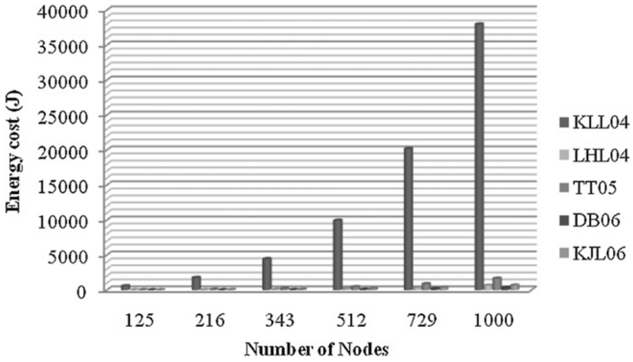

Fig. 28 – Total energy cost of two-round authenticated protocols based on hash functions.

Table 15 – Complexity analysis of two-round unauthenticated protocols.

Protocol	Number of exponentiations	Number of sent messages	Number of received messages
NCKW04 (Nam et al., 2004a)	$3n - 2$	$2n - 1$	$n^2 - 1$
T07b (Tseng, 2007b)	$3n - 2$	$2(n - 1)$	$n^2 - n$
ZGL10 (Zhao et al., 2010)	$3n^2 - n$	$n^2 + n$	$n^3 - n$
BD05 (Burmester and Desmedt, 2005)	$3n$	$2n$	$2n(n - 1)$
ZR04 (Zou and Ramamurthy, 2004)	n^2	n^2	$n^3 - n^2$
BRZV05 (Balachandran et al., 2005)	n^2	$2n$	$2n(n - 1)$
T05a (Tseng, 2005a)	$4n^2 + n$	$5n$	$5n(n - 1)$
ZW08 (Zhang and Wang, 2008)	$2n^2$	$n^2 + 2n$	$n^3 + n^2 - 2n$

communication cost. A medium communication cost is brought by protocols BRZV05 (Balachandran et al., 2005) and BD05 (Burmester and Desmedt, 2005), while protocols T07b (Tseng, 2007b) and NCKW04 (Nam et al., 2004a) display the best performance, in terms of communication.G The total energy cost of the least efficient of the protocols in question is depicted in Fig. 33. Protocols ZGL10 (Zhao et al., 2010), ZW08 (Zhang and Wang, 2008) and ZR04 (Zou and Ramamurthy, 2004) have the largest energy cost and this is a result of their very high communication cost. Moreover, protocol T05a (Tseng, 2005a) seems to have a relatively high total energy cost, but in this case, this comes mainly as a result of the protocol's computation cost. While it remains high, the total energy cost brought by protocol BRZV05 (Balachandran et al., 2005) is much better than the one of the aforementioned protocols. As for the remaining protocols, we present their total energy costs in Fig. 34. From Fig. 34, we can easily discern that T07b (Tseng, 2007b) and NCKW04 (Nam et al., 2004a) protocols are the most efficient unauthenticated protocols with T07b having a slightly better performance.

5.8. *Performance evaluation of Section 4.3.1.6 protocols*

In this subsection, we thoroughly examine and assess the performance of the two-round GKA protocols, which have been proposed in the literature in both their authenticated and their unauthenticated version. Table 16 summarizes the computations taking place during these protocols' execution and have negligible cost. Note that each protocol name is followed by number one (1), when we refer to the unauthenticated version of the protocol and by number two (2), when we refer to its authenticated version. The only exception is DL08 protocol (Desmedt and Lange, 2008), where DL08 (1) and DL08 (2) are unauthenticated protocols and DL08 (3) is

Table 14 – Computations having negligible cost of two-round unauthenticated protocols.

Protocol	Number of Encryptions	Number of Decryptions	Number of Hash functions	Number of Greatest Common Divisor computations
NCKW04 (Nam et al., 2004a)	–	–	n	–
ZGL10 (Zhao et al., 2010)	–	–	n^2	–
ZR04 (Zou and Ramamurthy, 2004)	$n(n - 1)$	$n(n - 1)$	–	–
BRZV05 (Balachandran et al., 2005)	–	–	–	n
T05a (Tseng, 2005a)	–	–	n^2	–

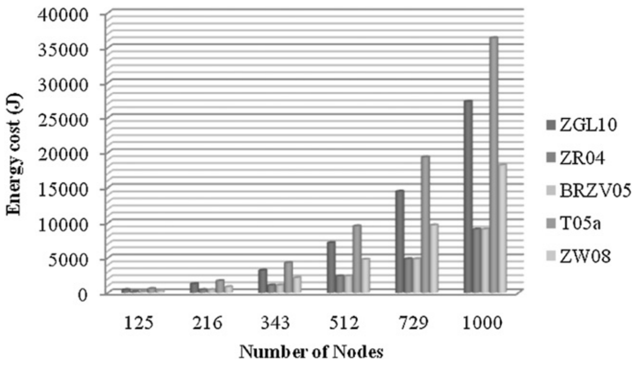

Fig. 29 – Computation cost of the least efficient two-round unauthenticated protocols.

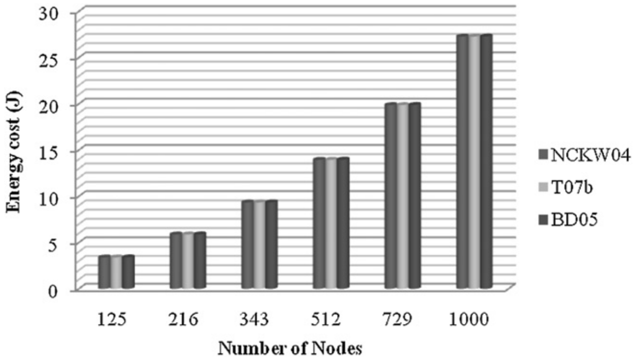

Fig. 30 – Computation cost of the most efficient two-round unauthenticated protocols.

the authenticated version of DL08 (2). Moreover, in D07 protocol (Dutta, 2007), the energy cost is equal for both the authenticated and unauthenticated version. In Table 17, we present the total computation and communication cost of the protocols. Based on this table, we have created the figures that follow. For the cost assessment of these protocols, we have divided them into two categories: the least efficient and the most efficient protocols.

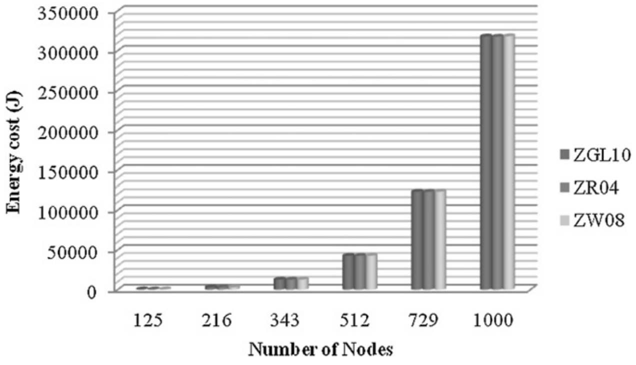

Fig. 31 – Communication cost of the least efficient two-round unauthenticated protocols.

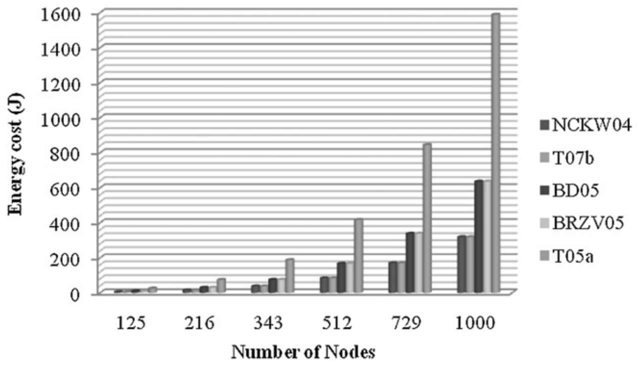

Fig. 32 – Communication cost of the most efficient two-round unauthenticated protocols.

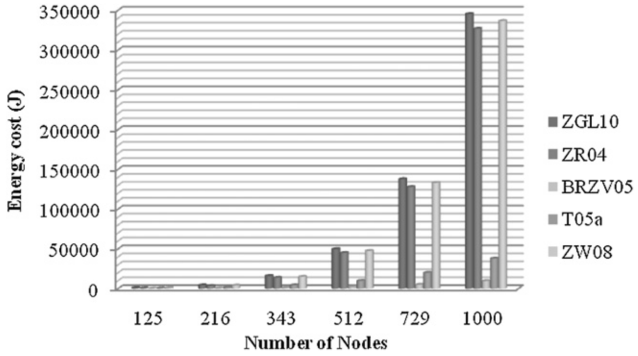

Fig. 33 – Total energy cost of the least efficient two-round unauthenticated protocols.

Figs. 35 and 36 present the computation cost of the examined protocols. In Table 17 we notice that the authenticated protocol DB05 (2) (Dutta and Barua, 2005a) has by far the highest computation cost, due to its square computational complexity. This protocol is the only protocol with square computational complexity, in this group, and that is the reason for the huge difference it has, with respect to the remaining protocols. Thus, we excluded it from the graphs that follow. In Fig. 35, it can be seen that protocols DL08 (3)

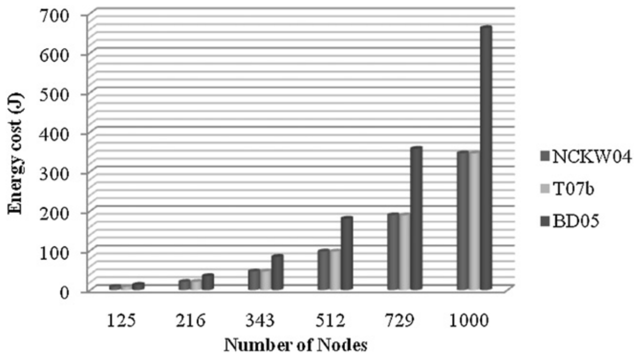

Fig. 34 – Total energy cost of the most efficient two-round unauthenticated protocols.

Table 16 – Computations having negligible cost of two-round authenticated and unauthenticated protocols.

Protocol	Number of Encryptions	Number of Decryptions	Number of Hash functions
D07 (Dutta, 2007)	$2n$	$n^2 + n$	–
LLT09 (2) (Lee et al., 2009)	–	–	n
CHL04 (2) (Choi et al., 2004)	–	–	$4n$

(Desmedt and Lange, 2008), CHL04 (2) (Choi et al., 2004) and LLT09 (Lee et al., 2009), in an ascending cost order, are the most energy consuming, in terms of computation, since we have excluded protocol DB05 (2) (Dutta and Barua, 2005a) from the comparison. A medium and identical computation cost is brought by both the authenticated and the unauthenticated protocol of LLC06 (Lin et al., 2006).

As we can see in Fig. 36, protocols CHL04 (1) (Choi et al., 2004), DL08 (1) and (2) (Desmedt and Lange, 2008) follow the abovementioned, least efficient protocols, while the most efficient protocols are DB05 (1) (Dutta and Barua, 2005a) and D07 (Dutta, 2007), with exactly the same computation cost. It is worth mentioning that the computation cost difference between the authenticated and unauthenticated version of DB05 protocol (Dutta and Barua, 2005a) is huge, which leads to the conclusion that the inclusion of authentication mechanisms in a protocol can be very costly.

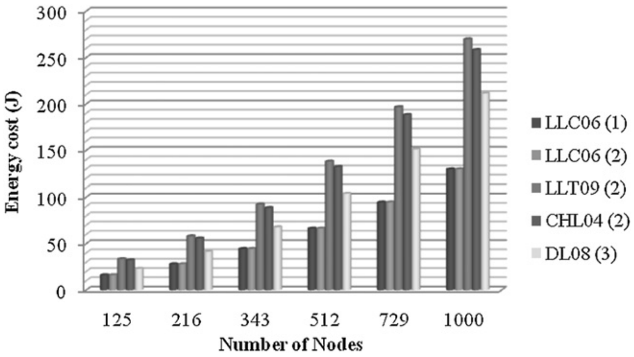

Fig. 35 – Computation cost of the least efficient two-round authenticated and unauthenticated protocols.

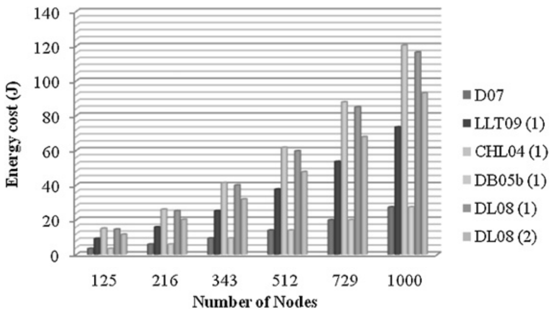

Fig. 36 – Computation cost of the most efficient two-round authenticated and unauthenticated protocols.

In Figs. 37 and 38, we can see the communication cost of the examined protocols. As it is obvious from Fig. 37, the worst performance is displayed by protocol DB05 (2) (Dutta and Barua, 2005a) followed by protocols D07 (Dutta, 2007) and DB05 (1) (Dutta and Barua, 2005a). More efficient than the previous ones, are protocols CHL04 (2) (Choi et al., 2004) and LLC06 (2) (Lin et al., 2006), which have the same communication cost. In Fig. 38, we notice that also CHL04 (1) (Choi et al., 2004) and LLC06 (1) (Lin et al., 2006) protocols have the same communication cost. In addition, very efficient protocols are the authenticated and unauthenticated versions of protocol LLT09 (Lee et al., 2009), with the former displaying a slightly higher communication cost. The most efficient protocols in this category are the three protocols presented in DL08 (Desmedt and Lange, 2008), with DL08 (2) and DL08 (3) having the best performance, in terms of communication. As it was expected from its high computation and communication cost, DB05 (2) protocol (Dutta and Barua, 2005a) displays the worst performance in overall. Hence, due to the huge cost difference between DB05 (2) (Dutta and Barua, 2005a) and the remaining protocols, we have excluded it from the total energy cost figures. In Fig. 39, we can see the total energy cost of the least efficient protocols. As it was expected, almost all protocols in

Table 17 – Complexity Analysis of two-round authenticated and unauthenticated protocols.

Protocol	Number of exponentiations	Number of pairings	Number of scalar multiplications	Number of sent messages	Number of received messages
LLC06 (1) (Lin et al., 2006)	$2n$	$2n$	$2n$	$2n$	$2n(n-1)$
LLC06 (2) (Lin et al., 2006)	$2n$	$2n$	$2n$	$3n$	$3n(n-1)$
D07 (Dutta, 2007)	$3n$	–	–	$3n-2$	n^2+2n-3
LLT09 (1) (Lee et al., 2009)	–	n	$3n-2$	$2n-2$	n^2-n
LLT09 (2) (Lee et al., 2009)	–	$5n-4$	$4n-2$	$3n-2$	n^2+n-2
CHL04 (1) (Choi et al., 2004)	–	$2n$	$3n$	$2n$	$2n(n-1)$
CHL04 (2) (Choi et al., 2004)	–	$4n$	$8n$	$3n$	$3n(n-1)$
DB05 (1) (Dutta and Barua, 2005a)	$3n$	–	–	$3n$	n^2+n
DB05 (2) (Dutta and Barua, 2005a)	$2n^2+7n$	–	–	$6n$	$2n^2+2n$
DL08 (1) (Desmedt and Lange, 2008)	$3n/2$	$2n$	n	$5n/2$	$n^2/2+2n$
DL08 (2) (Desmedt and Lange, 2008)	$3n/2$	$3n/2$	n	$7n/2$	$3n+n\log_4 n$
DL08 (3) (Desmedt and Lange, 2008)	$3n/2$	$3n/2$	$9n/2+2n\log_4 n$	$7n/2$	$3n+n\log_4 n$

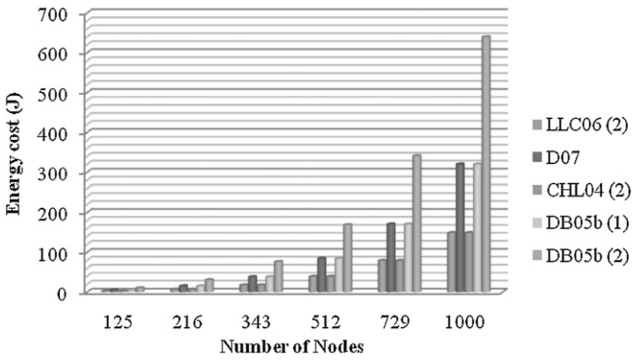

Fig. 37 – Communication cost of the least efficient two-round authenticated and unauthenticated protocols.

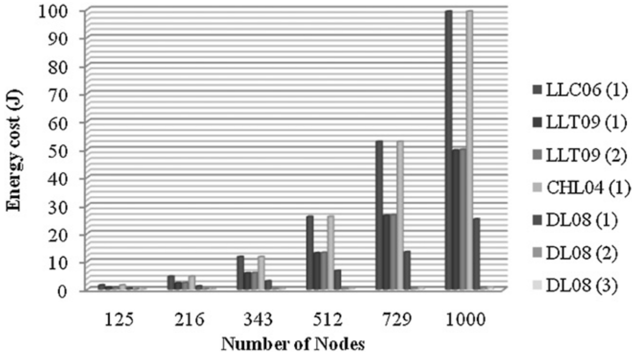

Fig. 38 – Communication cost of the most efficient two-round authenticated and unauthenticated protocols.

this figure are authenticated with the most efficient being LLC06 (2) (Lin et al., 2006). In Fig. 40, the most efficient protocols are displayed, which are all (except for DL08 (3) (Desmedt and Lange, 2008)) unauthenticated. It is concluded that the most efficient unauthenticated protocol is DL08 (2) (Desmedt and Lange, 2008), while the most efficient authenticated protocol is its counterpart DL08 (3) (Desmedt and Lange, 2008).

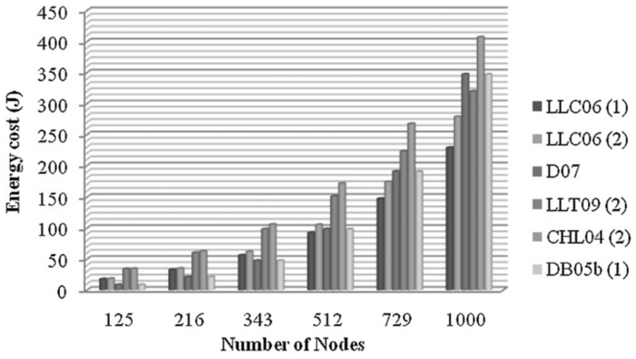

Fig. 39 – Total energy cost of the least efficient two-round authenticated and unauthenticated protocols.

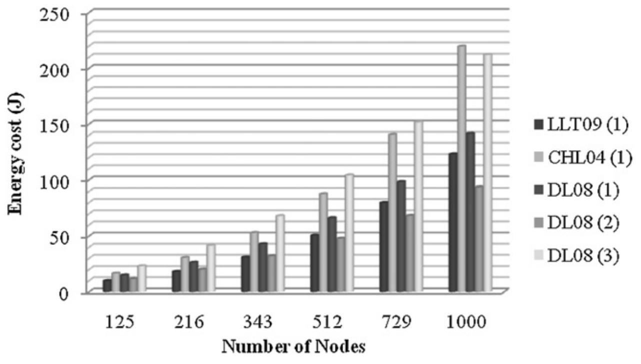

Fig. 40 – Total energy cost of the most efficient two-round authenticated and unauthenticated protocols.

5.9. *Performance evaluation of Section 4.4 protocols*

In this subsection we evaluate the performance of the one-round GKA protocols. In Table 18, we summarize the computations taking place during each protocol's execution and have negligible energy cost. In Table 19, we present the computation and communication complexity of the protocols. In the following figures, we have divided the protocols into two categories: the least efficient protocols and the most efficient protocols, in order to examine more carefully the differences among them.

In Fig. 41, we see that the worst performance, regarding the computation cost, is brought by protocol KKHY04 (Kim et al., 2004b). This is a result of the large number of pairings and scalar multiplications required. ZSM06 (1) (Zhou et al., 2006) and TT00 (1) (Tzeng and Tzeng, 2000) have similar performance, while XHX09 (Xia et al., 2009) has quite larger computation cost. In Fig. 42, we notice that BN03 (Boyd and Nieto, 2003) is by far the most efficient protocol, in computation terms, while SCL05 (Shi et al., 2005) and HH07 (He and Han, 2007) follow.

The communication cost of the one-round GKA protocols is presented in Figs. 43 and 44. Due to the enormous communication cost of protocols TT00 (1) (Tzeng and Tzeng, 2000), TT00 (2) (Tzeng and Tzeng, 2000) and ZSM06 (1) (Zhou et al., 2006), whose complexity of sent messages is square and the corresponding complexity of received messages is cubic, we present them separately in Fig. 43. The remaining protocols

Table 18 – Computations having negligible cost of one-round protocols.

Protocol	Number of Hash functions	Number of Pseudorandom functions
HH07 (He and Han, 2007)	$2n^2 - n$	–
KKHY04 (Kim et al., 2004b)	n^2	n
XHX09 (Xia et al., 2009)	$2n^2 - \mathrm{n}$	–
ZSM06 (1) (Zhou et al., 2006)	$3n^2 - 2n$	–
BN03 (Boyd and Nieto, 2003)	n	–
TT00 (Tzeng and Tzeng, 2000)	$3n$	–

Table 19 – Complexity Analysis of one-round protocols.

Protocol	Number of exponentiations	Number of pairings	Number of scalar multiplications	Number of sent messages	Number of received messages
SCL05 (Shi et al., 2005)	–	n	n^2	$n(n-1)$	$n(n-1)$
HH07 (He and Han, 2007)	–	$3n$	$3n^2$	$3n(n-1)$	$3n(n-1)$
KKHY04 (Kim et al., 2004b)	–	$4n^2-3n$	n^2+4n	$3n$	$3n(n-1)$
XHX09 (Xia et al., 2009)	–	n^2+n	$3n^2-2n$	$2n(n-1)$	$2n(n-1)$
ZSM06 (1) (Zhou et al., 2006)	–	$n(n-1)$	–	$n(n+1)$	n^3-n
BN03 (Boyd and Nieto, 2003)	$4n-3$	–	–	$2n-1$	$2n(n-1)$
TT00 (1) (Tzeng and Tzeng, 2000)	$5n^2+2n$	–	–	$n(2n+3)$	$2n^3+n^2-3n$
TT00 (2) (Tzeng and Tzeng, 2000)	$4n^2+n$	–	–	$2n^2+n$	$2n^3-n^2-n$

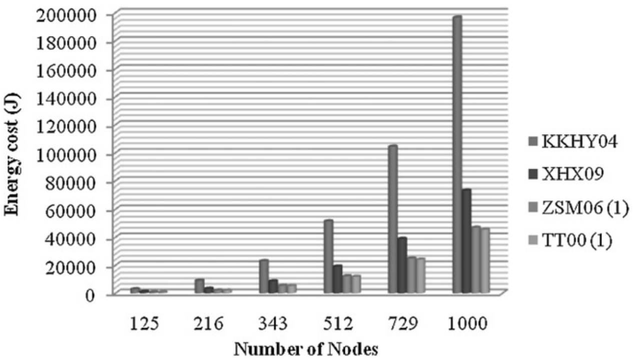

Fig. 41 – Computation cost of the least efficient one-round protocols.

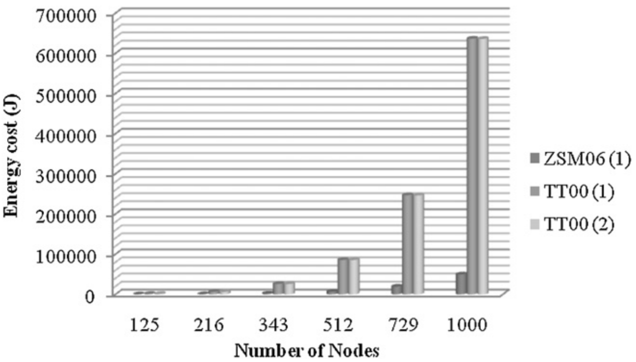

Fig. 43 – Communication cost of the least efficient one-round protocols.

have much smaller communication cost. From these protocols, as it is obvious from Fig. 44, the protocol that infers the higher cost is BN03 (Boyd and Nieto, 2003), followed by protocols HH07 (He and Han, 2007) and XHX09 (Xia et al., 2009). A much lower communication cost is brought by protocol SCL05 (Shi et al., 2005), while protocol KKHY04 (Kim et al., 2004b) has the best performance, in terms of communication.

Finally, Figs. 45 and 46 depict the total energy cost of the examined protocols. The enormous communication cost of TT00 (1) and TT00 (2) protocols (Tzeng and Tzeng, 2000), along with their relatively high computation cost, makes them inefficient and they are the most expensive protocols of this category (as we can see in Fig. 45). Also quite energy consuming is protocol KKHY04 (Kim et al., 2004b), followed closely by protocol ZSM06 (1) (Zhou et al., 2006). While the cost remains high, the performance of protocol XHX09 (Xia et al., 2009) is relatively better than the performance of the above-mentioned protocols and its total energy cost comes mainly as a result of its large computation cost. In Fig. 46, we observe that protocol HH07 (He and Han, 2007) has a medium total energy cost. An even better overall performance is displayed by protocol SCL05 (Shi et al., 2005). Finally, BN03 protocol (Boyd and Nieto, 2003), having a remarkable difference from the rest of the protocols, requires the least total energy for its execution. This is the result of the protocol's extremely low computation cost.

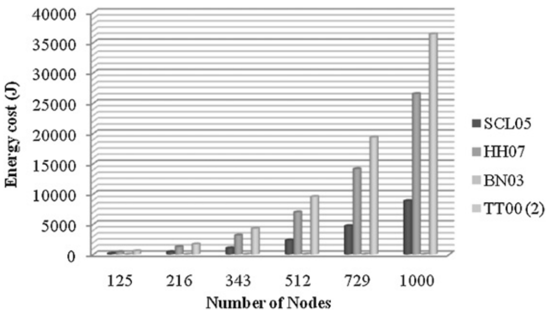

Fig. 42 – Computation cost of the most efficient one-round protocols.

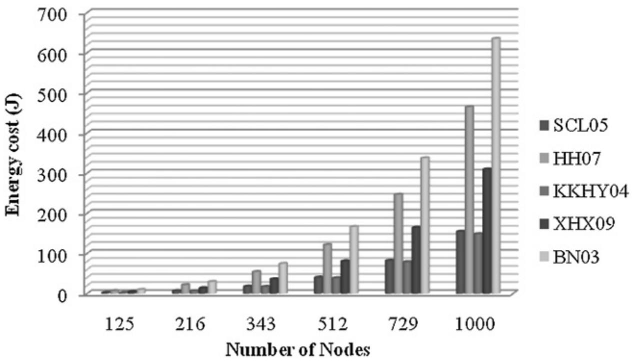

Fig. 44 – Communication cost of the most efficient one-round protocols.

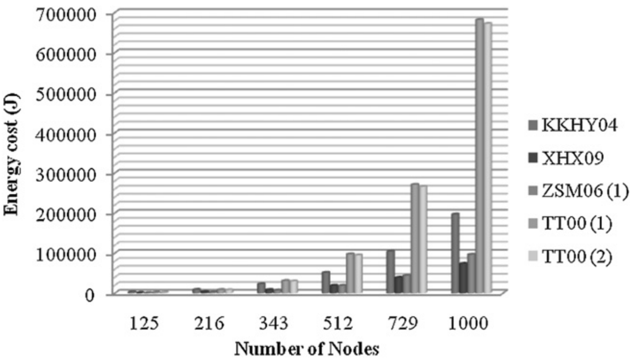

Fig. 45 – Total energy cost of the least efficient one-round protocols.

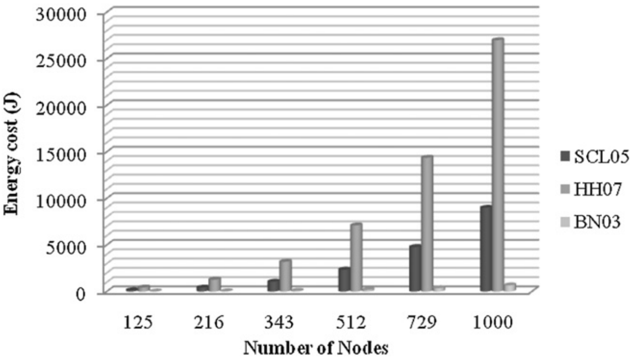

Fig. 46 – Total energy cost of the most efficient one-round protocols.

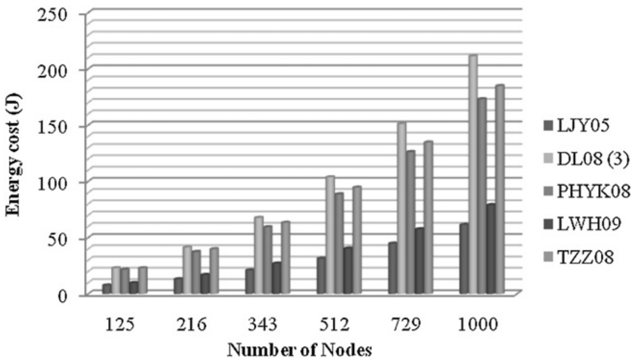

Fig. 47 – Computation cost of the top five authenticated protocols.

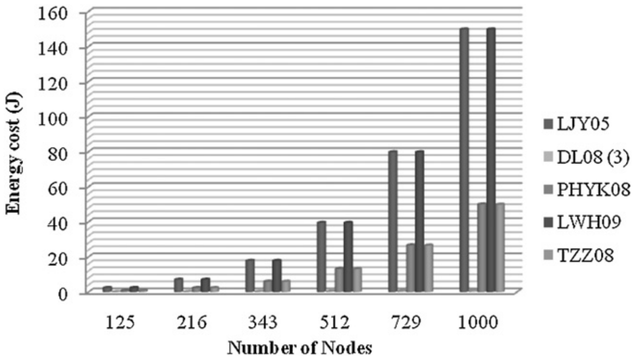

Fig. 48 – Communication cost of the top five authenticated protocols.

5.10. *Performance evaluation of the top five authenticated protocols*

In this subsection, we have collected the five constant round authenticated GKA protocols, with the best performance regarding their total energy cost. These protocols have already been examined, but they are going to be presented once more, in order to see more carefully how they are compared and point out the reasons of their efficiency. These five protocols are: LJY05 (Li et al., 2005), which is a two-round protocol based on ID-PKI, PHYK08 (Park et al., 2008), which is a three-round GKA protocol based on a KGC, LWH09 (Lu et al., 2009), which is a two-round GKA protocol based on the different computational capabilities of network nodes, TZZ08 (Tang et al., 2008), which is a two-round protocol based on a KGC and DL08 (3) (Desmedt and Lange, 2008), which is based on bilinear pairings. In Table 20, we present the total computation and communication cost of the top five authenticated GKA protocols. Notice that all of them display linear computational complexity.

In Fig. 47, the computation cost of these five authenticated constant round GKA protocols is presented. The most efficient protocol, in terms of computation, is LJY05 (Li et al., 2005), followed by LWH09 (Lu et al., 2009) (both of them do not require pairing computations). A higher computation cost is brought by protocol PHYK08 (Park et al., 2008), while the highest computation cost is inferred by protocols TZZ08 (Tang

Table 20 – Complexity analysis of the top five authenticated protocols.

Protocol	Number of exponentiations	Number of pairings	Number of scalar multiplications	Number of sent messages	Number of received messages
LJY05 (Li et al., 2005)	–	–	$7n$	$9n$	$3n^2 + 3n$
DL08 (3) (Desmedt and Lange, 2008)	$3n/2$	$3n/2$	$9n/2 + 2n \log_4 n$	$7n/2$	$3n + n \log_4 n$
PHYK08 (Park et al., 2008)	–	$2n + 2$	$9n$	$4n$	$n^2 + 2n$
LWH09 (Lu et al., 2009)	–	–	$9n + 1$	$7n + 3$	$3n^2 + 7n - 6$
TZZ08 (Tang et al., 2008)		$3n$	$5n$	$3n$	$n^2 + n$

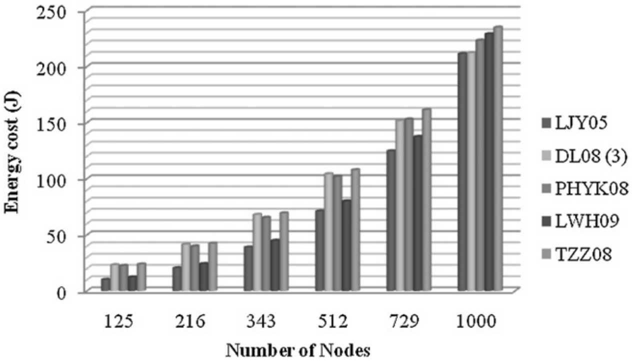

Fig. 49 – Total energy cost of the top five authenticated protocols.

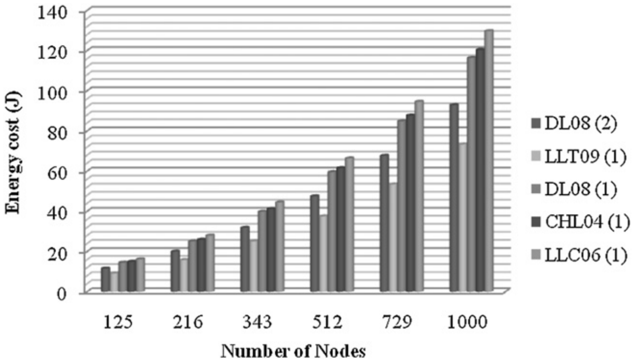

Fig. 50 – Computation cost of the top five unauthenticated protocols.

et al., 2008) and DL08 (3) (Desmedt and Lange, 2008), with the latter being the most expensive, in terms of computation.

Regarding the communication cost of the examined protocols, depicted in Fig. 48, LJY05 protocol (Li et al., 2005) has the worst performance, followed by LWH09 protocol (Lu et al., 2009). Protocols PHYK08 (Park et al., 2008) and TZZ08 (Tang et al., 2008), in an ascending order of performance, are very efficient in terms of communication, bringing a very similar cost. Finally, protocol DL08 (3) (Desmedt and Lange, 2008) has a really low communication cost, which makes its performance exceptional.

As for the total energy cost of the top five authenticated constant round GKA protocols, when the number of nodes used in the assessment is equal to 1000, the protocols appear in the following order: LJY05 (Li et al., 2005), DL08 (3) (Desmedt and Lange, 2008), PHYK08 (Park et al., 2008), LWH09 (Lu et al., 2009) and TZZ08 (Tang et al., 2008), as we can see in Fig. 49. Regardless of the number of network nodes, the most efficient protocol in overall is LJY05 (Li et al., 2005). However, for 729 network nodes, or less, protocol LWH09 (Lu et al., 2009) has the second best performance, instead of forth. As for DL08 (3) protocol (Desmedt and Lange, 2008), it comes forth for 512 network nodes or less, third for 729 network nodes and second for 1000 network nodes, a fact which proves the protocol's scalability and practicality, especially for a large number of protocol participants.

5.11. *Performance evaluation of the top five unauthenticated protocols*

In this subsection, we have collected the five constant round unauthenticated GKA protocols, with the best performance regarding their total energy cost. These protocols are secure against only passive attacks and in order to resist active attacks they should be transformed to authenticated ones, by proper mechanisms or compilers (which clearly increase their total energy cost). All protocols require two rounds and are the following: DL08 (1) and (2) (Desmedt and Lange, 2008), which are based on bilinear pairings, LLT09 (1) (Lee et al., 2009), which is based on the different computational capabilities of network nodes, CHL04 (1) (Choi et al., 2004), which is based on a KGC and LLC06 (1) (Lin et al., 2006), which is based on a Certification Authority. In Table 21, we summarize the computation and communication cost of these five unauthenticated GKA protocols.

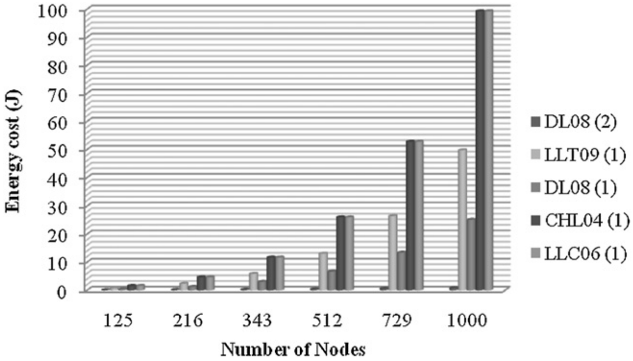

Fig. 51 – Communication cost of the top five unauthenticated protocols.

Figs. 50 and 51 present the protocols' total computation and communication cost, respectively. The highest computation

Table 21 – Complexity Analysis of the top five unauthenticated protocols.

Protocol	Number of exponentiations	Number of pairings	Number of scalar multiplications	Number of sent messages	Number of received messages
DL08 (2) (Desmedt and Lange, 2008)	$3n/2$	$3n/2$	n	$7n/2$	$3n + n\log_4 n$
LLT09 (1) (Lee et al., 2009)	–	n	$3n - 2$	$2n - 2$	$n^2 - n$
DL08 (1) (Desmedt and Lange, 2008)	$3n/2$	$2n$	n	$5n/2$	$n^2/2 + 2n$
CHL04 (1) (Choi et al., 2004)	–	$2n$	$3n$	$2n$	$2n(n - 1)$
LLC06 (1) (Lin et al., 2006)	$2n$	$2n$	$2n$	$2n$	$2n(n - 1)$

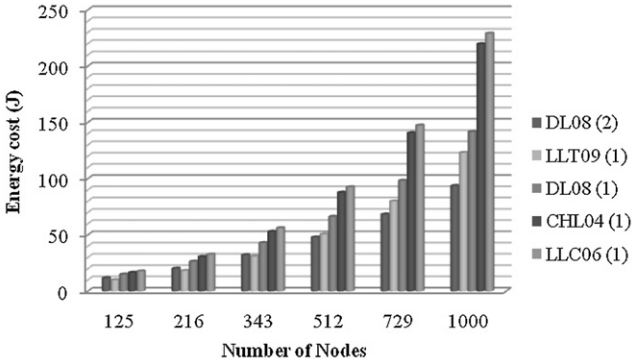

Fig. 52 – Total energy cost of the top five unauthenticated protocols.

cost is brought by protocol LLC06 (1) (Lin et al., 2006), while the most efficient protocol in terms of computation, is LLT09 (1) (Lee et al., 2009). Regarding the communication cost of the most efficient unauthenticated GKA protocols, DL08 (2) protocol (Desmedt and Lange, 2008) is by far the least costly. Protocol DL08 (1) (Desmedt and Lange, 2008) comes second, making both protocols presented in Desmedt and Lange (2008) the most efficient constant round protocols, proposed so far in the literature, regarding their communication cost. Protocols CHL04 (1) (Choi et al., 2004) and LLC06 (1) (Lin et al., 2006) have exactly the same communication cost, while much more efficient is LLT09 (1) protocol (Lee et al., 2009).

In Fig. 52, the total energy cost of the examined protocols is presented. The most efficient protocol for 512 network nodes, or more, is DL08 (2) protocol (Desmedt and Lange, 2008), but it comes second for 343 network nodes, or less. Moreover, protocol LLT09 (1) (Lee et al., 2009) is a very efficient protocol, being ranked at the first place for 343 network nodes, or less, and in the second place for 512 network nodes, or more. A comparatively medium total energy cost is inferred by protocol DL08 (1) (Desmedt and Lange, 2008), while the worst performance among the five protocols is displayed by protocols CHL04 (1) (Choi et al., 2004) and LLC06 (1) (Lin et al., 2006).

6. Conclusion

The ultimate goal of this survey is to present and evaluate the majority of the constant round GKA protocols proposed so far in the literature. We have briefly presented the main characteristics of each protocol and grouped them accordingly in several categories. The performance evaluation of the protocols was presented in appropriate tables and figures leading to interesting results on the efficiency of the protocols. Moreover, the evaluation of energy consumption for different group sizes offers a very useful insight into each protocol's scalability and practicality. Our detailed comparative study can serve as the basis for further evaluations and probably become the touchwood for the creation of new, more efficient GKA protocols.

REFERENCES

Abdalla M, Pointcheval D. A Scalable password-based group key exchange protocol in the standard model. Lecture Notes in Computer Science. In: Asiacrypt 2006, vol. 4284. Springer; 2006. pp. 332–347.

Abdalla M, Bresson E, Chevassut O, Pointcheval D. Lecture Notes in Computer Science. Password-based group key exchange in a constant number of rounds, in Public Key Cryptography 2006-PKC 2006, vol. 3958. Springer- Verlag; 2006. pp. 427–442.

Amir Y, Kim Y, Nita-Rotaru C, Tsudik G. On the performance of group key agreement Protocols. In: 22nd International conference on distributed computing systems (ICDCS), vol. 7. IEEE; 2004. Issue 3, pp. 463–464.

Augot D, Bhaskar R, Issarny V, Sacchetti D. A three round authenticated group key agreement protocol for Ad Hoc networks. Pervasive and Mobile Computing 2007;3(1): 36–52.

Avanzi RM, Cohen H, Doche C, Frey G, Lange T, Nguyen K, Vercauteren F. Handbook of elliptic and Hyperelliptic curve cryptography. Chapman and Hall/CRC; 2006.

Balachandran R, Ramamurthy B, Zou X, Vinodchandran N. CRTDH: An efficient key agreement scheme for secure group communications in wireless ad hoc networks. In: Communications 2005, ICC, IEEE International Conference, 2005, vol. 2. pp. 1123–1127.

Blake I, Seroussi G, Smart N. Elliptic curves in cryptography, London Mathematical Society Lecture note Series 265. Cambridge University Press; 1999.

Bohli JM, Steinwandt R. Deniable group key Agreement. Lecture Notes in Computer Science. In: Progress in Cryptology – VIETCRYPT 2006, vol. 4341. Springer; 2006. pp. 298–311.

Bohli JM, Glas B, Steinwandt R. Towards provably secure group key agreement building on group Theory. Lecture Notes in Computer Science. In: Progress in Cryptology – VIETCRYPT 2006, vol. 4341. Springer-Berlin; 2006a. pp. 322–336.

Bohli JM, Vasco MIG, Steinwandt R. Password-authenticated constant-round group key establishment with a common reference string. Cryptology ePrint Archive; 2006b. Report 2006/214.

Boyd C, Nieto JMG. Round-Optimal contributory conference key Agreement. Lecture Notes in Computer Science. In: Public key cryptography – PKC 2003, vol. 2567. Springer-Verlag; 2003. pp. 161–174.

Bresson E, Catalano D. Constant round authenticated group key agreement via distributed Computation. Lecture Notes in Computer Science. In: Public key cryptography 2004-PKC 2004, vol. 2947. Springer-Verlag; 2004a. pp. 115–129.

Bresson E, Catalano D. Constant round authenticated group key agreement from general Assumptions. In: CIRM research Center (Cryptography workshop). France: University of Marseille; November 8th–12th 2004b.

Bresson E, Chevassut O, Pointcheval D, Quisquater J-J. Provably authenticated group Diffie-Hellman key exchange. In: ACM Conference on Computer and Communications security – CCS 01, 2001. pp. 255–264.

Burmester M, Desmedt Y. Lecture Notes in Computer Science. A secure and efficient conference key distribution system (Extended Abstract), Eurocrypt 1994, vol. 950. Springer-Verlag; 1994. pp. 275–286.

Burmester M, Desmedt Y. A secure and Scalable group key exchange system. Information Processing Letters 2005;94(3): 137–43.

Cao CJ, Ma JF. Identity-based constant round group key exchange protocol via secret-Share. WSEAS Transactions on Systems 2008;7(1):7–16.

Challal Y, Seba H. Group key management protocols: a novel taxonomy. International Journal of Information Technology 2005;2(1):105–19.

Cho S, Nam J, Kim S, Won D. An efficient dynamic group key agreement for low-power mobile Devices. Lecture Notes in Computer Science. In: International conference on computational Science and its applications – ICCSA 2005, vol. 3480. Springer; 2005. pp. 99–112.

Cho H, Kim GS, Eom Y. Partial Group Session Key Agreement Scheme for Mobile Agents in e-Commerce Environment. Lecture Notes in Computer Science. In: Agent computing and multi-Agent systems, vol. 4088. Springer; 2006. pp. 420–431.

Cho S, Song K, Cho D, Won D. Secure mobile Content Delivery using dynamic group key agreement with batch Verification. Lecture Notes in Computer Science. In: Computational Science and its applications – ICCSA 2007, vol. 4706. Springer-Verlag; 2007. pp. 996–1007.

Choi KY, Hwang JY, Lee DH. Efficient ID-based group key agreement with bilinear Maps. Lecture Notes in Computer Science. In: Public key cryptography 2004-PKC 2004, vol. 2947. Springer-Verlag; 2004. pp. 130–144.

Choi KY, Hwang JY, Lee DH. Id-based authenticated group key agreement secure against insider attacks. In: IEICE Transactions on fundamentals of electronics. Communcations and Computer Sciences, E91-A; 2008. p. 1828–30.

Cramer R, Shoup V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen LR, editor. Eurocrypt 2002. Lecture notes in Computer Science, vol. 2332. Berlin, Germany: Springer-Verlag; 2002. pp. 45–64.

Desmedt Y, Lange T. Lecture Notes in Computer Science. Revisiting pairing based group key exchange, in Financial cryptography and data security, vol. 5143. Springer-Berlin; 2008. pp. 53–68.

Du X, Wang Y, Ge J, Wang Y. An ID-Based authenticated two round multi-party key agreement. Cryptology ePrint Archive; 2003a. Report 2003/247.

Du X, Wang Y, Ge J, Wang Y. An improved ID-based authenticated group key agreement scheme. Cryptology ePrint Archive; 2003b. Report 2003/260.

Dutta R, Barua R. Constant round dynamic group key agreement, vol. 3650. Springer; 2005a. Lecture Notes in Computer Science74–88.

Dutta R, Barua R. Overview of key agreement protocols. Available at:. Cryptology ePrint Archive <http://eprint.iacr.org/2005/289>; 2005b. Report 2005/289.

Dutta R, Barua R. Password-based encrypted group key agreement. International Journal of Network Security 2006;vol. 3(1):30–41. Also available at: <http://isrc.nchu.edu.tw/ijns>.

Dutta R, Barua R. Provably secure constant round contributory group key agreement in dynamic Setting. IEEE Transactions on Information Theory 2008;54(5):2007–25.

Dutta R, Barua R, Sarkar P. Pairing-based cryptography: a survey. Cryptology ePrint Archive; 2004. Report 2004/064.

Dutta R. Multi-Party key agreement in password-based Setting. In: First Asia International conference on Modelling & Simulation – AMS 2007. IEEE; 2007. p. 133–8.

Feng T, Wang Y, Ma J. A secure and efficient group key agreement for ad hoc networks. International Symposium on Computer Science and Computational Technology 2008;2:540–3.

Fu X, Xu Q, Wang H. A provably-secure password-authenticated group key agreement in the standard model. Journal of Networks 2009;4(8):763–70.

Geng M, Zhang F, Gao M. A Secure Certificateless Authenticated Group Key Agreement Protocol. In: International Conference on Multimedia Information Networking and Security, 2009, vol. 1, pp. 342–346.

Gennaro R, Lindell Y. A framework for password-based authenticated key exchange. Available at: In: Biham E, editor. Eurocrypt 2003. Lecture notes in Computer Science, vol. 2656. Berlin, Germany: Springer-Verlag. p. 524–43 <http://eprint.iacr.org/2003/032.ps.gz>; 2003.

Gorantla MC, Boyd C, Gonzalez Nieto J, Manulis M. Generic one round group key exchange in the standard Model. Lecture Notes in Computer Science. In: 12th International conference on information security and Cryptology – ICISC 2009, vol. 5984. Springer; 2009. pp. 1–15.

He YZ, Han Z. An efficient authenticated group key agreement protocol. In: 41st Annual IEEE International Carnahan Conference on Security Technology, 2007, pp. 250–254.

He YZ, Li XY, Han Z. An insider attack resistant group key agreement protocol from pairings. In: International Journal of innovative computing, information and Control – ICICIC 2007. IEEE; 2007.

Hu C, Liu P, Li D. An Efficient Group Key Agreement Protocol from Bilinear Pairings. In: International Conference on Computational Intelligence and Security Workshops, 2007, pp. 737–740.

Jarecki S, Kim J, Tsudik G. Robust group key agreement using short broadcasts. In: 14th ACM Conference on Computer and Communications security – CCS, 2007, pp. 411–420.

Jiang B, Hu X. A Survey of Group Key Management. In: International Conference on Computer Science and Software Engineering, 2008, vol. 3, pp. 994–1002.

Just M, Vaudenay S. Authenticated multi-party key agreement. Lecture Notes in Computer Science. In: Advances in Cryptology – Asiacrypt 1996, vol. 1163. Springer-Verlag; 1996. pp. 36–49.

Katz J, Yung M. Scalable protocols for authenticated group key exchange. In: Boneh D, editor. Crypto 2003. Lecture notes in Computer Science, vol. 2729. Berlin, Germany: Springer-Verlag; 2003. pp. 110–125.

Kim J, Tsudik G. Survival in the Wild: robust group key agreement in wide-area networks. Lecture Notes in Computer Science. In: Information security and Cryptology – ICISC 2008, vol. 5461. Springer-Heidelberg; 2008. pp. 66–83.

Kim HJ, Lee SM, Lee DH. Constant-round authenticated group key exchange for dynamic groups. Lecture Notes in Computer Science. In: Advances in Cryptology – ASIACRYPT 2004, vol. 3329. Springer-Verlag; 2004a. pp. 127–140.

Kim JS, Kim HC, Ha KJ, Yoo KY. One round identity-based authenticated conference key agreement protocol. Lecture Notes in Computer Science. In: ECUMN 2004, vol. 3262. Springer-Verlag; 2004b. pp. 407–416.

Kim H, Nam J, Kim S, Won D. Secure and efficient ID-based group key agreement fitted for pay-TV. Lecture Notes in Computer Science. In: The Pacific-Rim conference on multimedia PCM 2005, vol. 3768. Springer-Berlin; 2005. pp. 117–128.

Klaoudatou E, Konstantinou E, Kambourakis G, Gritzalis S. A survey on cluster-based group key agreement protocols for WSNs. Available at: In: IEEE communications surveys and Tutorials. IEEE Press <http://dl.comsoc.org/surveys>; 2010.

Kwon JO, Jeong IR, Lee DH. Provably-Secure two-round password-authenticated group key exchange in the standard Model. Lecture Notes in Computer Science. In: IWSEC 2006, vol. 4266. Springer; 2006. pp. 322–336.

Lee SM, Hwang JY, Lee DH. Efficient password-based group key exchange. Lecture Notes in Computer Science. In: 1st International conference on Trust and privacy in digital Business – TrustBus 2004, vol. 3184. Springer-Verlag; 2004. pp. 191–199.

Lee SM, Lee SY, Lee DH. Efficient group key agreement for dynamic TETRA Networks. Lecture Notes in Computer Science. In: Theory and practice of Computer Science – SOFSEM 2007, vol. 4362. Springer-Verlag; 2007. pp. 400–409.

Lee C, Lin T, Tsai C. A new authenticated group key agreement in a mobile environment. Annals of Telecommunications 2009; 64(11). pp. 735–744.

Li X, Jiang X, Ye C. An Effective Constant-Rounds Group Key Exchange for Dynamic Groups. In: 5th International Conference on Information, Communications and Signal Processing, 2005, pp. 443–447.

Li L, Tsai Y, Liu R. A novel ID-based authenticated group key agreement protocol using bilinear pairings, in 5th IFIP International Conference on Wireless and Optical Communications Networks, 2008-WOCN, 2008, pp. 1–5.

Lin CH, Lin HH, Chang JH. Multiparty Key Agreement for Secure Teleconferencing. In: IEEE International Conference on Systems, Man and Cybernetics – ICSMC, 2006, vol. 5, pp. 3702–3707.

Lu C, Wu T, Hsu C. Certificateless authenticated group key agreement protocol for Unbalanced wireless mobile networks. WSEAS Transactions on Communications 2009; 8(11):1145–59.

Lv X, Li H. ID-based authenticated group key agreement from bilinear maps. Frontiers of Computer Science China 2010;4(2): 302–7.

Manulis M. Security-Focused Survey on Group Key Exchange Protocols, Technical Report. In: Cryptology ePrint Archive, Report 2006/395, 2006. Available at: <http://eprint.iacr.org/2006/395>.

McCullagh N, Barreto PSLM. A New two-party identity-based authenticated key Agreement. Lecture Notes in Computer Science. In: Proceedings of CT – RSA 2005, vol. 3376. Springer-Verlag; 2005. pp. 262–274.

Merwe JVD, Dawoud D, Mcdonald S. A survey on peer-to-peer key management for mobile ad hoc networks. ACM Computing Surveys – CSUR 2007;39(1):1–45.

Nam J, Cho S, Kim S, Won D. Simple and efficient group key agreement based on Factoring. Lecture Notes in Computer Science. In: Computer Science and its applications – ICCSA 2004, vol. 3043; 2004a. pp. 645–654.

Nam J, Kim S, Kim S, Won D. Provably-Secure and communication-efficient scheme for dynamic group key exchange. Available at: Cryptology ePrint Archive <http://eprint.iacr.org/2004/115>; 2004b. Report 2004/115.

Nam J, Kim S, Yang H, Won D. Secure group communications over Combined Wired/Wireless networks. Available at: Cryptology ePrint Archive <http://eprint.iacr.org/2004/260.pdf>; 2004c. Report 2004/260.

Nam J, Lee J, Kim S, Won D. DDH-based group key agreement in a mobile environment. Systems and Software 2005;78(1):73–83.

Nam J, Paik J, Kim UM, Won D. Constant-Round authenticated group key exchange with logarithmic computation Complexity. Lecture Notes in Computer Science. In: Applied cryptography and network security – ACNS 2007, vol. 4521. Springer-Heidelberg; 2007. pp. 158–176.

Park H, Han K, Yeun CY, Kim K. Improving Choi et al.'s ID-based Authenticated Group Key Agreement Scheme at PKC2004. In: Symposium on Cryptography and Information Security, Japan, 2008.

Park H, Asano T, Kim K. Improved ID-based Authenticated Group Key Agreement Secure Against Impersonation Attack by Insider. In: Symposium on Cryptography and Information Security, Japan, 2009.

Pereira O. Modelling and security analysis of authenticated group key agreement protocols, Ph.D thesis, Universite Catholique de Louvain, 2003.

Rafaeli S, Hutchison D. A survey of key management for secure group communication. Journal of the ACM Computing Surveys – CSUR 2003;35(3):309–29.

Saha M, Chowdhury DR. A conference key agreement protocol for mobile environment. Journal of Information Assurance and Security 2009a;4:60–8.

Saha M, Chowdhury DR. A secure and efficient protocol for group key agreement in heterogeneous environment, arXiv:0908.2509v1 [cs.CR]. Available at: <http://arxiv.org/PS_cache/arxiv/pdf/0908/0908.2509v1.pdf>; 2009b.

Schnorr CP. Efficient signature generation for smart cards. Journal of Cryptology 1991;4(3):239–52.

Shi Y, Chen G, Li J. ID-Based One Round Authenticated Group Key Agreement Protocol with Bilinear Pairings. In: International Conference on Information Technology: Coding and Computing – ITCC, 2005, vol. 1, pp. 757–761.

Silverman J. The arithmetic of elliptic curves. Springer-Verlag; 1986.

Tan CH, Teo JCM. An Authenticated Group Key Agreement for Wireless Networks. In: IEEE Wireless Communications and Networking Conference 2005-WCNC, 2005, vol. 4, pp. 2100–2105.

Tan CH, Teo JCM. Energy-efficient ID-based group key agreement protocols for wireless networks. In: 20th International Parallel and Distributed Processing Symposium, 2006-IPDPS, 2006, pp. 25–29.

Tang H, Zhu L, Zhang Z. Efficient ID-Based Two Round Authenticated Group Key Agreement Protocol, in 4th International Conference on Wireless Communications, Networking and Mobile Computing – WiCOM, 2008, pp.1–4.

Tseng YM. A robust multi-party key agreement protocol resistant to malicious participants. Computer Journal 2005a;48(4):480–7.

Tseng YM. An improved conference-key agreement protocol with forward secrecy. In: Informatica, 2005, vol. 16. IOS Press; 2005b. Issue 2, pp. 275–284.

Tseng YM. A communication-efficient and fault-tolerant conference-key agreement protocol with forward secrecy. Journal of Systems and Software 2007a;80(7):1091–101.

Tseng YM. A resource-constrained group key agreement protocol for imbalanced wireless networks. Computers and Security 2007b;26(4):331–7.

Tseng YM. A secure authenticated group key agreement protocol for resource-limited mobile devices. Computer Journal 2007c; 50(1):41–52.

Tso R, Yi X, Okamoto E. ID-Based Key Agreement for Dynamic Peer Groups in Mobile Computing Environments. In: 2nd IEEE Asia-Pacific Services Computing Conference, 2007, pp. 103–110.

Tzeng WG, Tzeng ZJ. Round-efficient conference-key agreement protocols with provable security. Lecture Notes in Computer Science. In: Advances in Cryptology – ASIACRYPT 2000, vol. 1976. Springer-Berlin; 2000. pp. 614–627.

Tzeng WG. A secure fault-tolerant conference key agreement protocol. IEEE Transactions on Computer 2002;51(4):373–9.

Wan Z, Ren K, Lou W, Preneel B. Anonymous id-based group key agreement for wireless networks. In: IEEE Wireless Communications and Networking Conference, 2008 – WCNC, 2008, pp. 2615–2620.

Wu S, Zhu Y. Constant-Round password-based authenticated key exchange protocol for dynamic Groups. Lecture Notes in Computer Science. In: 12th International conference on Financial cryptography and data security – FC 2008, vol. 5143. Springer; 2008. pp. 69–82.

Wu B, Wu J, Cardei M. A survey of key management in mobile ad hoc networks. In: Zheng J, Zhang Y, Ma M, editors. Handbook of research on wireless security, vol. 2; 2007. pp. 479–499.

Xia M, He M, Xie L. A New ID-based group key agreement protocol for the network. Journal of Computational Information Systems 2009;5(6):1855–60.

Yao G, Wang H, Jiang Q. An Authenticated 3-Round Identity-Based Group Key Agreement Protocol. In: 3rd International Conference on Availability, Reliability, and Security – ARES, 2008, pp. 538–543.

Yeun CY, Han K, Vo DL, Kim K. Secure authenticated group key agreement protocol in the MANET environment. Information Security Technical Report 2008;13(3):158–64.

Yi X. Identity-Based fault-tolerant conference key agreement. IEEE Transactions on Dependable and Secure Computing 2004; 1(3):170–8.

Zhang F, Chen X. Attack on an ID-based authenticated group key agreement scheme from PKC 2004. Information Processing Letters 2004;91:191–3.

Zhang J, Varadharajan V. Wireless sensor network key management survey and taxonomy. Journal of Network and Computer Applications 2010;33(2):63–75.

Zhang XI, Wang QM. An improved conference key agreement protocol. International Conference on Computational Intelligence and Security 2008;2:314–8.

Zhang H, Wen Q, Zhang J, Li W. A constant rounds group key agreement protocol without using hash functions. International Journal of Network Management 2009;19(6): 457–64.

Zhang L, Wu Q, Qin B, Domingo-Ferrer J. Identity-Based authenticated asymmetric group key agreement Protocol. Lecture Notes in Computer Science. In: Computing and Combinatorics, vol. 6196. Springer; 2010. pp. 510–519.

Zhao J, Gu D, Li Y. An efficient fault-tolerant group key agreement protocol. Computer Communications 2010;33(7):890–5.

Zheng S, Wang S, Zhang G. A dynamic, secure, and efficient group key agreement protocol. Frontiers of Electrical and Electronic Engineering in China 2007;2(2):182–5.

Zheng MH, Zhou HH, Li J, Cui GH. Efficient and provably secure password-based group key agreement protocol. Computer Standards & Interfaces 2009;31(5):948–53.

Zhou L, Susilo W, Mu Y. Efficient ID-Based authenticated group key agreement from bilinear Pairings. Lecture Notes in Computer Science. In: Mobile ad hoc and sensor networks – MSN 2006, vol. 4325. Springer-Verlag; 2006. pp. 521–532.

Zou X, Ramamurthy B. A simple group Diffie-Hellman key agreement protocol without member serialization. Lecture Notes in Computer Science. In: Computational and information Science – CIS 2004, vol. 3314. Springer-Verlag; 2004. pp. 725–731.

Zou X, Thukral A, Ramamurthy B. An authenticated key agreement protocol for mobile ad hoc networks. Lecture Notes in Computer Science. In: Mobile ad hoc and sensor networks – MSN 2006, vol. 4325. Springer; 2006. pp. 509–520.

Elisavet Konstantinou holds a B.Sc. in Informatics from the University of Ioannina, a M.Sc. in Signal and Image Processing Systems and a PhD in Theory and Applications of Elliptic Curve Cryptosystems from the University of Patras, Department of Computer Engineering and Informatics. She is currently an Assistant Professor in the Department of Information and Communication Systems Engineering, University of the Aegean. Her research interests include elliptic curves cryptosystems and generation of their parameters, public key cryptosystems, group key management, random number generation, algorithm engineering, algebraic number theory.

Eleftheria Makri received her B.Sc. in Informatics from the Technological Educational Institute of Athens, School of Technological Applications (2009), and her M.Sc. in Information & Communication Systems Security from the University of the Aegean, School of Engineering (2011). Her scientific interests lie in the field of key agreement and key management as well as in wireless network security and intrusion detection systems.