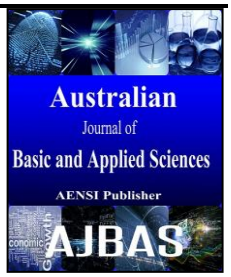
Australian Journal of Basic and Applied Sciences, 9(16) Special 2015, Pages: 204-210

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com



A Provision of Secure Group Communication and Reduced Overheads in Grid Circumstances

Dr. N.M. Saravanakumar and S. Lavanya

Associate Professor, Department of CSE, Bannari Amman Institute of Technology, Sathyamangalam
Assistant Professor, Department of IT, Sri Krishna College of Engg. and Technology, Coimbatore

ARTICLE INFO

Article history:
Received 20 January 2015
Accepted 02 April 2015
Published 20 May 2015

Keywords:
Group Key, communication, computation Complexity, Security as a service, group communication.

ABSTRACT

Due to heterogeneous, geographically distributed grid resources, it belongs to different administrative domains. Overheads and security is a major concern in a grid system. Several multi-party systems supporting group- and cloud-based applications have been proposed in the context of Smart Grid. The requirement of these systems is that the applications or devices need to communicate with each other as a group. This paper presents a one-cost overhead complexity in order to reduce the computation and communication overhead and securing the group communications. It follows the group/cluster-based approach to reduce the costs of the SGK (Sub-Group Key) construction and maintenance for large groups. The evaluation tools in the technical community shows that our constructed SGK is valid and secure against well-known attacks

To Cite This Article: Dr. N.M. Saravanakumar and S. Lavanya, A Provision of Secure Group Communication and Reduced Overheads in Grid Circumstances. ***Aust. J. Basic & Appl. Sci.,*** *9(16): 204-210, 2015*

INTRODUCTION

Grid Computing deals with coordinated way of sharing diverse resources that are available in distributed "Virtual Organizations". There are two important functions in grid such as communication and resource sharing. In grid computing, group communication is an important issue to realize large-scale information resource sharing. However, it is very difficult to ensure the security of group communication in large-scale grid environment. Since the grid collaboration happens by means of the Internet and since the Internet is not security – oriented by design, there is a possibility of many attacks, in particular malicious internal and external users or hackers. Two important requirements in grid include the formation of virtual organizations (VO) dynamically and establishment of secure communication between the grid entities. A VO is a dynamic group of individuals, groups, or organizations that have common rules for resource sharing (Foster, 2001).

Security in computational grids serves authentication, authorization, non-repudiation, integrity, confidentiality and auditing. To eliminate the unauthorized users from visiting the grid resources strong mutual authentication between grid entities should be assured. Confidentiality of information in a VO should also be ensured (Von Welch). The necessity for secure communication between grid entities has motivated the development of the Grid Security Infrastructure (GSI). GSI operate at the transport layer requires an ordered reliable transport connection, so it is implemented over Transmission

Control Protocol (TCP), hence this approach is not suitable for web service-based technologies.

The proposal in (Xukai Zoua, 2007) is an Dual-Level Key Management (DLKM) mechanism using Access Control Polynomial (ACP) and one-way functions. This scheme provides flexibility and hierarchical access control thereby it secures the group communication.

The identity-based authentication protocol for grid is based on the identity-based architecture for grid (IBAG) and corresponding encryption and signature schemes were also experimented. It is being certificate-free, the authentication protocol aligned well with the demands of grid computing has been proposed in (Li Hongweia).

The concept in (Yan Zhenga) uses an identity-based signature (IBS) scheme for grid authentication and analysis in (Hai-yan 2007) gives a grid authentication mechanism based on combined public key (CPK) which employs elliptic curve cryptography (ECC). To ensure secure communication, key distribution occurs between the grid entities and grid entities are authenticated once.

Corresponding Author: Dr. N.M. Saravanakumar, Associate Professor, Department of CSE, Bannari Amman Institute of Technology, Sathyamangalam

The protocol presented in (Wang,2011) is an extension of the existing protocol called S-3PAKE, both of which construct the GK assuming the existence of a server. The protocol of increases the number of users of the group from three to n. In both protocols, the server plays the main role by receiving messages from all users and then responds to the users. Since the server needs to provide services to the entire usership and is involved in all the steps in the interaction, the protocol is vulnerable to the single point of failure.

By utilizing Exclusion Basis Systems (BES) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) techniques in [9], a GK management for large scale systems is proposed. It provides an EBS-Based protocol that supports forward/backward secrecy relative to the join/leave process, and resilience to collusion attacks. Instead of using a clustering approach, it uses CP-ABE to handle large groups, which is more useful for the multicast communications.

Identity-Based Cryptography (IBC) is used in (Mailloux, 2011) to design a GK agreement for multicast communications. The design maintains forward secrecy and integrity, and is developed for a dynamic environment. The system requires a group leader with whom each user communicates to prepare the shared values for the key construction. Although the process consists of two rounds, in each round communication with the leader is required.

The protocol proposed in (Teng, 2012) is based on identities and do not require certificates. The protocol starts by each user choosing a random number and sending it to other users. Then, the results of the second round calculations are broadcast to all the users. The users are able to compute the GK after the second round. Similar to many other proposals, this protocol relies on broadcasting data/messages to others, which may not be robust for large groups.

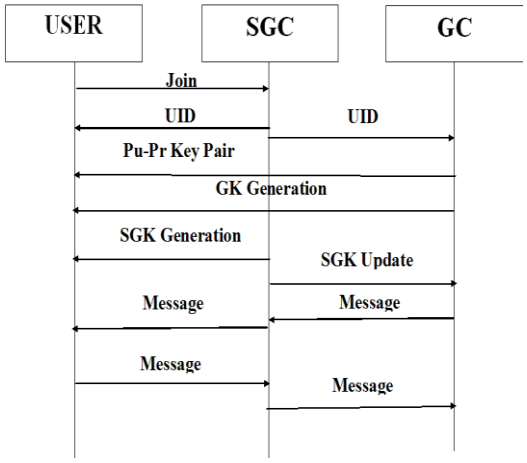


Fig. 1: Process of the Proposed Methodology.

Several IBC-based GK agreement protocols are evaluated in (Konstantinou, 2011). Moreover, a survey on security of group communications is presented in (Sakarindr, 2010). A brief survey on cluster-based GK Agreement (GKA) protocols for wireless sensor networks is presented in (Klaoudatou, 2011), differentiated into infrastructure-based and infrastructure-less networks. The infrastructure-based protocols studied include the Hierarchical Key Agreement Protocol, GKA protocol for Circular Hierarchical Group, Password-Based GKA protocol for Hierarchical Group and AP-1 which is a cluster-based GKA protocol based on the constant round multi-party dynamic key agreement protocol. The survey shows that the best performance is delivered in a system with equal cluster size and a small number of layers.

The proposal in (Sun, 2010) provides a GK management for the advanced distribution automation system of SG, which is based on a three-tier tree structure and decentralized architecture. In (Kamto,2011), firstly a SG gateway constructs a symmetric key with each SM based on a D-H algorithm. Then, the gateway multiplies the symmetric keys to form a GK, and finally, sends the GK using the symmetric keys to the SMs.

The tree concept is used in the key management proposal in (Jung-Yoon, 2012) to cover unicast, multicast and broadcasting keys for the SG, in which the multicast key is close to our design. The design is based on a binary tree in which each node uses two hash functions to calculate secret values of the tree nodes, which requires knowing the entire tree construction. Due to the high resource consumption and overhead cost, it may not be suitable for the SG with many nodes.

The proposed work aims at authenticating the users and reducing the overheads in terms of storage, communication and computation overhead. The remaining of the paper is organized as follows: Section 2 is constituted by the proposed mechanism. Section 3 discusses about the analysis done so far. Section 4 discusses about implementation results and Section 5 concludes the paper.

Proposed method:

Initially VO assigns the number of sub-groups (cluster) to be constructed based on resource or storage to which the users are grouped. For instance we consider the number of sub-groups under VO to be 3 as shown in figure 1 where *SGC1*, *SGC2*, and *SGC3* are sub-groups. Let there be 8 users with who are to be grouped under *SGC1*, 2 users under *SGC2*, and 2 users under *SGC3*.

Step 1: Generation of UID to indicate presence of users in a group.

Step 2: Generation of Group Key (GK) and Sub-Group Key (SGK) used for inter and intra group communication.

Step 3: Generation of Public-Private Key (Pu-Pr key) and Signature used to provide
security services.

UID is assigned to each user in the group. If a user joining any one of the group and the SGC generates UID and transmit to the user. Then SGC send corresponding UID to VO, then VO generates Pu-Pr key, signature for the newly joined user. Using UID, users can access the resources and using GK, SGK, Pu-Pr key authentication, integrity is ensured.

Finally communication takes place between SGK and the user to use the grid resources. The methodology of the proposed scheme is shown in figure 1.

A. Generation of UID:

In this scheme, UID is used to identify the user in the group and it is used to know what distributed resource is used by the user in the grid. UID for each user in the sub-group is generated using prime factor. Consider k is a UID where k=1,2,3,4,…n is the primitive factor of α where α is a prime integer as shown in table 1.

Table I : Uuid Generation.

S.No	α	k	UID
1	5	2	2
2	7	3	3
3	13	6	6
4	16	5	5
5	17	10	10
6	31	17	17
7	43	28	28
8	53	26	26
9	67	12	12
10	71	62	62

Likewise, the UID generation goes on. The same primitive roots come, the SGC has to eliminate it and find the new key for each user in a group. This UID has been removed and never been reused for any other user in a group.

Analysis:

Before the *UID* generation under any Sub-group. A simple sorting operation requires minimum *N* number of comparisons and maximum N^2 where *'N'* is the number of users. Further, *UID*s are generated using prime factors. It operates in *O(N)* time where the sorting takes *O(N log N)* times. Sorting is to specify the number has been used already.

B. Sub-group Key and Group Key Generation:

a) *Generate sub-group Keys using Partial Keys from Users*: Each user under a sub-group sends the partial key, $f^{L_{1,1}}$ to *SGC*, where *i = 1, 2, 3, 4, ...* and *j = 1, 2, 3, ...* The SGC then uses these partial keys to compute the sub-group keys (*SGK*s). Here, f is the generator of the multiplicative group, Z_N^* which is the set *1, 2,..., N − 1, N* is the prime and *L* is a randomly chosen prime number for respective user. For example, from Figure 2, *SGC1* gets $f^{L_{1,1}L_{2,1}L_{3,1}L_{4,1}}$. Then each *SGC* adds its own partial key, f^{K_j} where *j = 1, 2, 3, ..,* and computes the sub-group key. i.e. *SGC1* adds its partial key say, f^{K1}. The resulting sub-group key of *SGC1* is given by Equation 1.

$$SGK_1 = f^{L_{1,1}L_{2,1}L_{3,1}L_{4,1}L_{5,1}L_{6,1}L_{7,1}L_{8,1}K_1} \quad (1)$$

The resulting *SGK* is sent to each user and is used for encryption and decryption of the message exchange among the users within the sub-group.

b) *Generate Group Keys using the Partial Keys from SGCs*: The VO collects the partial key of each sub- group. Consider Figure 2. Let partial keys of *SGC*s be f^{K1}, f^{K2} and f^{K3} respectively. The VO receives f^{K1K2K3} and the group key, *GK* is computed by VO by adding its own partial keys as shown in Equation 2.

$$GK = f^{K_1K_2K_3K_{GC}} \quad (2)$$

Here, GK is constant and hence SGK varies for each join and leave operation.

Analysis:

Let the number of Sub-group Controllers (SGCs) under VO be *C* and number of users under any SGC be N_i, where, *i=1,2…C*. The VO uses the partial keys received from each SGC and also its own partial key to generate *GK*. Hence it takes *O(log C+1)* operations for GK generation. In the same way, SGC uses partial keys of its users and also its own to generate SGK. Hence it takes *O(log N+1)* operations for SGK generation.

C. Public-Private keys and Signature Generation:

Each user is given long-term public and private keys. The VO randomly chooses a secret key and the computes and publishes the corresponding public key. SEGKMS uses the idea of RSA to construct a private-public key pair, where the VO calculates (1) public key *(M, E)*, where *M* is the product of any two large prime numbers, *a* and *b*, and *E* is the number

prime with respect to *M* and (2) private key *(a, b, d, φ(M))*, where *d* is the part of private key of VO and is equal to e^{-1} *mod φ(M).* The VO determines a primitive element *α* in *GF(a)* and *GF(b).* Then it chooses a one-way hash function. Here, *(α, h())* is a public information where *h()* gives unique output for different input. Each *SGC* provides *UID*s of the user under it to the VO to obtain the signature $S_{i,j}$ for each $UID_{i,j}$ of a user $m_{i,j}$, where *i = 1, 2, 3, ...*, represents each user and *j = 1, 2, or 3* represents the *SGC*. If VO confirms the correctness and the relationship between $m_{i,j}$ and $UID_{i,j}$, then it calculates $S_{i,j}$ using Equation 3 and distributes $S_{i,j}$ to each *SGC* where each *SGC* distributes them to the respective users.

$$S_{i,j} = UID_i^d \bmod M \quad (3)$$

Both public-private keys pair and signatures are distributed using proactive secret sharing scheme.

Analysis:

RSA concept is used for public-private key generation. If *K* is the number of bits in modulus *M* then public key operations takes $O(K^2)$ steps and private key operations take $O(K^3)$ steps.

D. Communication:

Finally, communication happens between the users.Let us know how any two users, $u_{i,j}$ and $u_{k,j}$, communicate with each other.

1) $u_{i,j}$ selects a random number $R_{i,j}$ and computes two public keys $x_{i,j}$ and $y_{i,j}$ as follows:

$$x_{i,j} = S_{i,j}.\alpha^{R_{i,j}} \bmod M \quad (4)$$

$$y_{i,j} = R_{i,j}^e \bmod M \quad (5)$$

2) $u_{i,j}$ uses a timestamp $T_{i,j}$ and the identification number $UID_{k,j}$ of the user $u_{k,j}$ for the operation of one-way function of $h(x_{i,j}, y_{i,j}, T_{i,j}, UID_{i,j})$, then computes

$$P_{i,j} = S_{i,j}.R_{i,j}^{h(x_{i,j}, y_{i,j}, T_{i,j}, UID_{k,j})} \bmod M \quad (6)$$

3) $u_{i,j}$ sends $(UID_{k,j}, x_{i,j}, y_{i,j}, T_{k,j})$ to $UID_{k,j}$.

Similarly, user $u_{k,j}$ selects the random number $R_{k,j}$ and the timestamp $T_{k,j}$, then computes $x_{k,j}$, $y_{k,j}$, and $P_{k,j}$ i.e.

$$P_{k,j} = S_{k,j}.R_{k,j}^{h(x_{k,j}, y_{k,j}, T_{k,j}, UID_{i,j})} \bmod M \quad (7)$$

and sends $(UID_{k,j}, x_{k,j}, y_{k,j}, T_{k,j})$ to $UID_{i,j}$. Each user sends this information through the *SGC*s. Before session key (*SK*) generation, $UID_{i,j}$ and $UID_{k,j}$ have to verify whether $(UID_{k,j}, x_{i,j}, y_{i,j}, T_{k,j})$ and $(UID_{k,j}, x_{k,j}, y_{k,j}, T_{k,j})$ are sent from users $m_{i,j}$ and $m_{k,j}$ respectively. It is done by checking

$$P_{k,j}^e = UID_{k,j}.y_{k,j}^{h(x_{k,j}, y_{k,j}, T_{k,j}, UID_{i,j})} \bmod M \quad (8)$$

Consider $P_{k,j}$ from Equation 8. From Equation 7,

$$P_{k,j}^e = (UID_{k,j}^d \bmod M)^e.(R_{k,j}^{h(x_{k,j}, y_{k,j}, T_{k,j}, UID_{i,j})} \bmod M)^e$$

Mathematically, $(G^x \bmod n)^y = (G^y \bmod n)^x = G^{xy} \bmod n$ and $(G^x \bmod n) \bmod n = (G^x \bmod n)$ because n is a very large number. According to RSA, $d = e^{-1} \bmod \varphi(n)$ and $d * e = 1 \bmod \varphi(n) = 1$

$$P_{k,j}^e = UID_{k,j}.y_{k,j}^{h(x_{k,j}, y_{k,j}, T_{k,j}, UID_{i,j})} \bmod M$$

which is similar to Equation 9. Similarly, user verify at his end that

$$P_{k,j}^e = UID_{i,j}.y_{i,j}^{h(x_{i,j}, y_{i,j}, T_{i,j}, UID_{k,j})} \bmod M \quad (9)$$

The communicating users compute a secret session key (*SK*). The computation of *SK*s is as follows: Consider the communication between two users $u_{i,j}$ and $u_{k,j}$. They compute the secret *SK*s i.e., $SK_{i,j}$ and $SK_{k,j}$ respectively as follows (Teng, 2012):

$$SK_{i,j} = \left(\frac{x_{k,j}^e}{UID_{k,j}}\right)_{k,j}^R \bmod M \quad (10)$$

$$SK_{k,j} = \left(\frac{x_{i,j}^e}{UID_{i,j}}\right)_{i,j}^R \bmod M \quad (11)$$

$SK_{i,j}$ and $SK_{k,j}$ are the same for the communicating users. Hence,

$$SK_{i,j} = SK_{k,j} = \alpha^{e*R1*R2} \bmod M \quad (12)$$

Since, M is a very large, the above equation can be written as

$$SK_{i,j} = SK_{k,j} = \alpha^{e*R1*R2} \quad (13)$$

Using these session keys, the users communicate successfully with each other.

E. Key Maintenance:

Key refreshment:

To improve and guarantee/increase the secrecy of the SGK, refreshes the key periodically. In order to do this, we propose rekeying where users join/leave the group, the key is changed on the application. Therefore, the following Sub-Group Key is reconstructed using the same formula in section 2.2. The system controller distributes a new SGK.

Join and leave process:

A new user should not gain access to the past information (forward secrecy), and a leaving user should not gain access to the future information (backward secrecy). In the case of a new user joining the existing group, or an existing user leaving the group, the controller performs calculation of new SGK to support the forward and backward secrecies.

Malicious behavior of a node:

In case one of the group users begins behaving maliciously, the malicious user is removed from the group. The system controller consists of UID of the existing and leaving member in the database so that the misbehaving user can be identified easily. In this case, they directly send a unicast message via the secure channel to the system controller. Subsequently, the system controller invokes the SGK generation algorithm for the group while excluding the malicious one.

Analysis of the proposed scheme:

In communication cost, whenever a user leaves or joins, there is a change database which is notified to sub-group controller once for each change. Hence, only one message is sufficient for any change in the network. The number of messages exchanged at any change in a group 1. It contains data about the users left/joined and the current status of the sub-group. Then the computation cost goes up to *O(1).*

In computation cost, when a user joins the group, the sub-group key is regenerated and along with the UID, Public-privates keys pair and signature for newly joined user. For each newly joining user three new keys and one UID is generated. If there are *k* users joining at the same time, then *4k* computations are done. Here *K* is a constant for any number of users since it depends only on the users joining or leaving but not on the users in the sub-group. Whenever a user leaves the group, only the *SGK* is regenerated. Hence, if *n* users are leaving the group, *n* times the *SGK* is generated. If they leave at the same time, only one *SGK* is regenerated. If joining and leaving are occurred at the same time, the number of computations done is only 1.

For Storage requirements, single user stores just three keys but the VO (server) stores *n+ 1* keys.

Rekeying message needed for join is 4 and the leave is only one.

Implementation and Discussion:

Table II: Comparison of parameters

	Communication Cost	Computation cost	Key Storage	Rekeying Message needed
Join	1	1	n+1	4
Leave	*1*	*1*	3	1

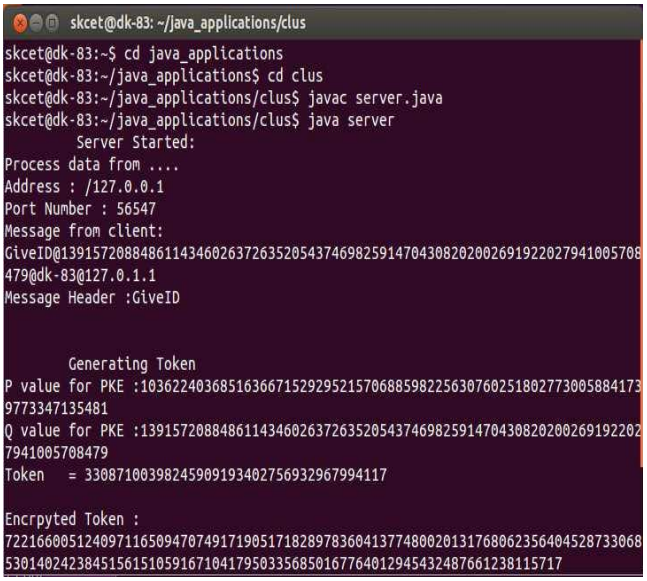


Fig. 2: Virtual Organization.

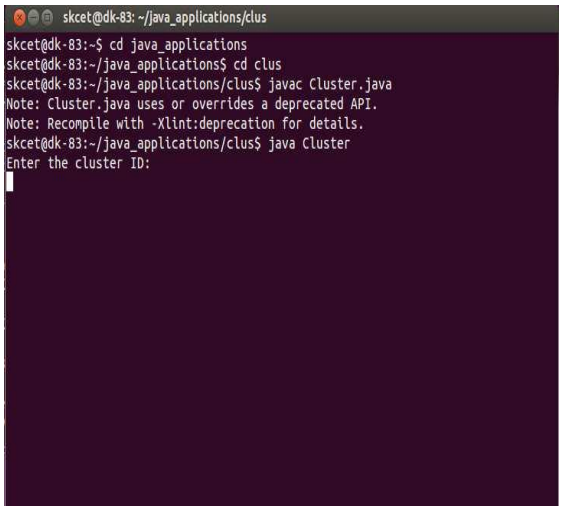


Fig. 3: Static Cluster/Group.

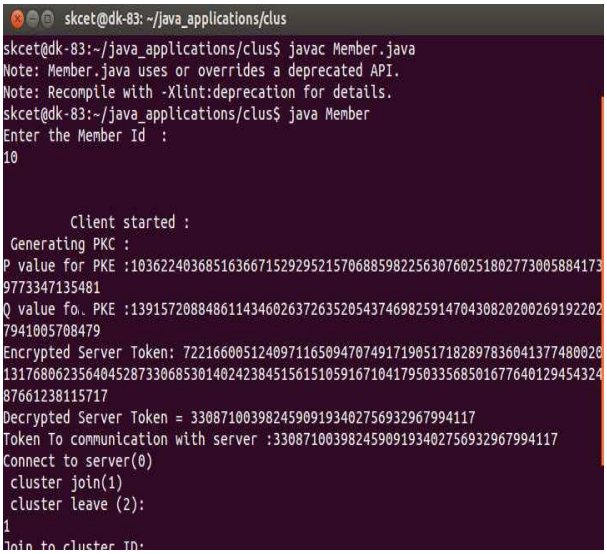


Fig. 4: Users Join/Leave.

Table III: Hash value table.

P Value	Q Value	Signature/Token	Encrypted Hash
1036224036 8516366715 2929521570 6885982256 3076025180 2773005884 1739773347 135481	13915720884 86114346026 37263520543 74698259147 04308202002 69192202794 1005708479	33087100398245 90919340275693 2967994117	722166005124097116509470749171 9051718289783604137748002013176 8062356404528733068530140242384 5156151059167104179503356850167 7640129454324876612381157
1573654062 0977670531 0417224788 0490089486 1197303450 2882362616 2298945837 651823	15036471699 83882084626 56758605634 81956966647 72490415789 02345258091 8545068293	68220043441531 62105523192767 5091209679	79813518389298574350468253875 76741793252373687251797851218 48572786760527353098594786343692 21551242254654835850363417

The proposed authentication and distribution of channels has been implemented and tested using java as shown in table 3 and on globus middleware. it is tested with twenty valid and users. Three of them are shown below with each of the valid users has their own identity, public-private key pair, signature/token. Initially, they have created their user account using uid (table 1). As the hash values used in the verification step ensures uniqueness and data integrity and confidentiality.

Conclusion:

In grid infrastructure, it is a systematic approach for the key management between the application to achieve a great advantage in terms of scalability, forward secrecy, backward secrecy, key independence, etc. The number of sub-groups is constant and SGK is dynamic to ensure secrecies hence the group key remains same throughout. The implementation of our system showed its effective performance in pinpointing the adversaries and paving the way to valid users to access resources in the VO by establishing as efficient computational channel distribution. Thus we achieved one cost in communication and computation overhead and improved security during communication.

REFERENCES

Chen, Y., G. Yang, 2011. Efficient and Secure Group Key Management Based on EBS and Attribute Encryption, in Proc. IEEE CSAE, Nanjing, China, Jun.

Foster, I., C. Kesselman and S. Tuecke, 2001. “The Anatomy of the Grid: Enabling Scalable Virtual Organizations”, International Journal of High Performance Computing Applications”, 15(3): 200-222.

Hai-yan Wanga, C. and Ru-chuan Wanga, 2007. "CPK-based grid authentication: a step forward",The Journal of China Universities of Postsand Telecommunications, 14(1): 26-31.

Jung-Yoon, K., C. Hyoung-Kee, 2012. An Efficient and Versatile Key Management Protocol for Secure Smart Grid Communications, in Proc. IEEE WCNC, Paris, France, Apr.

Kamto, J., L. Qian, J. Fuller, J. Attia, 2011. Light-Weight Key Distribution and Management for

Advanced Metering Infrastructure, in Proc. IEEE SG-COMNETS, Houston, TX, Dec.

Klaoudatou, E., E. Klaoudatou, G. Kambourakis, S. Gritzalis, 2011. A Survey on Cluster-Based Group Key Agreement Protocols for WSNs, IEEE Communication Surveys & Tutorials, 13(3): 429-442.

Konstantinou, E., E. Klaoudatou, P. Kamparmpakis, 2011. Performance Evaluation of ID-based Group Key Agreement Protocols, in Proc. 6th ARES, Vienna, Austria, Aug.

Li Hongweia, Sun Shixina and Yang Haomiaoa, "Identity-based authentication protocol for grid",Journal of Systems Engineering and Electronics, 19(4): 860-865.

Mailloux, N., A. Miri, M. Nevins, 2011. Forward Secure Identity-based Key Agreement for Dynamic Groups, in Proc. 9th PST, Montreal, QC, Jul.

Sakarindr, P., N. Ansari, 2010. Survey of security services on group communications, IET Information Security, 4(4): 258-272.

Sun, Z., J. Ma, 2010. Efficient Key Management for Advanced Distribution Automation System, in Proc. IEEE ICNIDC, Beijing, China, Sep.

Teng, J., C. Wu, 2012. A Provable Authenticated Certificateless Group Key Agreement with Constant Rounds, Journal of Communications and Networks, 14(1): 104-110.

Vijayakumar, V. and R.S.D. Wahida Banu, 2008. "Security for Resource Selection in Grid Computing Based On Trust and Reputation Responsiveness", IJCSNS International Journal of Computer Science and Network Security, 8(11).

Von Welch, Frank Siebenlist, Ian Foster, John Bresnahan, Karl Czajkowski, Jarek Gawor, Carl Kesselman, Sam Meder, Laura Pearlman and Steven Tuecke, "Security for Grid Services", in proceedings of the 12th IEEE International Symposium on High Performance Distributed Computing, pp: 48- 57.

Wang, M., J. Pan, J. Wang, Password-based Group Authenticated Key Exchange Protocol: From 3-Party to Group, in Proc. IEEE NCIS, Guilin, China, May 2011.

Xukai Zoua, Yuan-Shun Dai and Xiang Rana, 2007. "Dual-Level Key Management for secure grid communication in dynamic and hierarchical groups", Future Generation Computer Systems, 23(6): 776-786.

Yan Zhenga, Hai-yan Wanga and Ru-chuan Wang, "Grid authentication from identity-based cryptography without random oracles", The Journal of China Universities of Posts and Telecommunications, 15(4): 55-59.