Journal of Computer Science 7 (6): 917-923, 2011
ISSN 1549-3636

An Efficient Certificate-Free Key Distribution Protocol for Secure Group Communication in Grid Environment

Mandadi Venkatesulu and Kamatchi Kartheeban
Department of Computer Applications, Kalasalingam University, India

Abstract: Problem statement: In grid environment, group communication is an important mechanism to realize large-scale information resource sharing. However providing security for group communication in grid environment is very difficult because the group is dynamic in nature. Scalable group re-keying is one of the important issues in secure group communication. These group keys should be updated whenever a member joins/leaves the group to maintain the forward and backward secrecy. **Approach:** In the recent years, cryptography in grid environment plays an important role that allows secure group communication among members in the dynamic group. **Results:** Our algorithm for key distribution falls into NP-class. Therefore the key distribution is safe. **Conclusion:** Performance of the proposed algorithm is computationally efficient and cryptographically strong for message generation and key distribution.

Key words: Secure group communication, secure communication, proposed approach, modular polynomial, registration process, dynamic group, hierarchical groups, access control

INTRODUCTION

In recent years, due to the rapid growth of the internet, along with the availability of high-speed network and powerful computers as a low cost computing device is changing the mechanism of managing the information and information services. These new technologies have enabled to group a wide variety of geographically distributed heterogeneous resources like supercomputers, storage systems, sensors, visualization tools ,data sources, instruments and special devices , services and more, spreading across multiple administrative domains with the objective of providing users easy access to these resources as a unified resource. The new paradigm that has been evolved is popularly called as “Grid” computing.

Grid computing connects computers that are scattered over a geographic area allowing their computing power to be shared just as the World Wide Web enables access to information; computer grids enable access to computing resources. Thus, grids can combine the resources of thousands of different computers to create a massively powerful computing resource, accessible from the comfort of a personal computer and useful for multiple applications in science, business and beyond. Grid applications are distinguished from traditional client-server applications by their simultaneous use of massive amount of resources with dynamic requirements. Such resources are typically drawn from multiple administrative domains interconnected by complex communication structures and need to be accessed with stringent performance requirements. 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 organizations, individuals that have common rules for resource sharing.

Security in computational grids consists of authentication, authorization, non-repudiation, integrity, confidentiality and auditing. Confidentiality of information in a VO should also be ensured. The necessity for secure communication between grid entities has motivated the development of the Grid Security Infrastructure (GSI)-the defacto security standard in the grid community. The Grid Security Infrastructure (GSI) of the Globus Toolkit (GT) plays an essential role in supporting various grid security services such as single sign-on, mutual authentication, integrity, protection, confidentiality and delegation for sensitive information transferred over the network in addition to the facilities to securely traverse the distinct organizations that are part of collaboration. Being based on Public Key Infrastructure (PKI), GSI users are required to possess and manage long-term credentials (typically RSA public/private key pairs) which are usually renewed yearly. But however, GSI suffers from many potential security drawbacks such as uncontrolled

Corresponding Author: Mandadi. Venkatesulu, Department of Computer Applications, Kalasalingam University, India

delegation, leaky infrastructure and insecure services. Thus, further security mechanisms are needed to complement GSI in order to ensure the security of grid services. In grid environment, members or user applications may need access to resources that belong to different organizations. To work in grid environment the members in these organizations must form a group. Members in the grid group, before accessing resources that belong to different organizations should authenticate themselves. Once the grid entities are authenticated, key distribution occurs between the grid entities to ensure secure communication In order to perform secure group communications, security mechanism such as authentication, access control, integrity and confidentiality are required. Most of the mechanisms are generally based on encryption using one or several keys. The management of these keys including creating, distributing and updating the keys constitutes a basic block to build secure group communication system. In group communication confidentiality requires that only the members of the grid group could decrypt the message and get the key even if the message is broadcasted to the entire grid network.

The confidentiality requirements can be further classified into four key distribution rules.

Forward secrecy: Should ensure users who left the group should not have access to any future key.

Backward secrecy: Should ensure that a new user who joins the group should not get any access to the previous work.

Non-group confidentiality: Must ensure that users that were never part of the group should not have access to any key.

Collusion freedom: Should ensure that intruders should not be able to deduce the currently used key.

There are many more secure strategies and mechanism to ensure the security of grid such as ID authentication, authority and single sign-on. Confidentiality in information transfer in a distributed system is enabled by encrypting the information. Keys should be distributed securely among the members of the group. In existing approaches, each member shares a secret key with the group controller. If the information is to be transferred to 'k' members, 'k' encryptions followed by 'k' uncast are needed. The computational complexity of the existing approach is overcome by using encrypted session keys. Hence the proposed approach uses only an encrypting key with message followed by a multicast operation. This leads to reduced computation and provides efficient group communication. Further, the proposed approach ensures dynamic and secure group communication, forward secrecy and backward secrecy. The encrypted key is used to manage member join, leave operations efficiently. Since a key is maintained/generated for each group member join/leave, secure group communication is facilitated. The computation time of the message distribution along with the key and key derivation from the public message is fast when compared to the key distribution by traditional algorithms like AES.

In this study, we discuss the use of cryptography for secure key distribution in the dynamic grid environment. Also we introduce a mechanism for group key management in grid environment. The algorithms are analyzed with sample examples. The security analysis of the proposed scheme, conclusion and future research work in this direction are presented.

MATERIALS AND METHODS

To achieve security in grid, some technologies have been used to build security mechanism for grid computing. In order to avoid unauthorized users to make use of the grid resources a strong authentication is required between grid entities. Since password-based authentication is simple it has been used extensively in grid environment. Sudha *et al*. (2009) have proposed secret keys multiplication protocol based on modular polynomial arithmetic (SKMP), which eliminates the need for the encryption/decryption during the group re-keying. Valli *et al*. (2010) have proposed a new technique (SGKP-1), using hybrid key trees, has certain advantages like secure channel establishment for the distribution of the key material, reducing the storage requirements and burden at each member, minimization of time requirement to become a new member of a group. The computational complexity further reduced using both the combination of public and private key crypto systems. Xukai *et al*. (2007) have proposed an elegant Dual-Level key Management (DLKM) mechanism using Access Control Polynomial (ACP) and one-way hash functions. In this the first level provides flexible and secure group communication and the second level provides hierarchical access control. Park *et al*. (2010) have proposed an ID-based key distribution scheme which is secure against session state reveal attacks and long-term key reveal attacks. Also, our scheme offers the scalability, non-usage of additional cryptographic algorithms and efficiency similar to those of the existing schemes. Li1 *et al*. (2008a) have proposed reconcilable key management mechanism in which the key management middleware in grid can dynamically call the optimum re-keying algorithm and re-keying interval is based on the group members joining or leaving rate. Li1 *et al*. (2008b) Li *et al*. (2009) have proposed an authenticated encryption mechanism for group communication in terms of the basic theory of threshold signature and the basic characteristics of group communication in grid. In this approach each group member in the grid can verify the identity of the signer and hold the private key. Ingle and Sivakumar (2010) have proposed an Extended Grid Security Infrastructure (EGSI) to support secure group communication in grid and also present an authentication and access control scheme at virtual organization level. Zhenga *et al*. (2008) have proposed the use of Identity-Based Signature (IBS) scheme for grid authentication Hongweia *et al*. (2008) have proposed certificate-free identity-based authentication protocol for grid based on Identity-Based Architecture for Grid (IBAG) and by using corresponding encryption and signature scheme. Amir *et al*. (2008) have proposed that secure key management in hierarchical group communication by means of using intelligent agents that makes the architecture more flexible and dynamic preparing it for grid computing technologies. Purusothaman *et al*. (2010) have proposed cluster based hierarchical key distribution protocol for secure group communication. This approach uses prime number addition for member joining and leaving. Li *et al*. (2009) has proposed the service infrastructure of middleware for pervasive grid. Then, we present a secure mechanism of group communication and analyze the correctness and the security of the mechanism. Finally, we verify the validity of this mechanism by experiments

Key computation protocol: it is assumed that every valid user/machine/entity in the grid system is assigned a permanent secret identity, denoted by SID_i for member M_i. For example, when a member or an organization is willing to join the grid, they can join the grid only by doing registration with the globus toolkit. During this registration process several certificates need to be issued, including the host certificate that authenticates the machine involved in the grid, the service certificate that authenticates the services offered to the grid and the user certificates that are used to authenticate the use of the grid services. Also each member or a node in the grid system is allotted a permanent secret identity, denoted by SID_i for each member/node/machine M_i. During these registration process, the secret identity can be embedded into the certificates issued to the member.

Prime Number Based (PNB) Group Key Generator: Whenever there is a group of users participating in a grid service, the Key Distribution Manager (KDM) will generate the message M as follows:

Step1: Consider there are N members in the grid systems $N= (M_1, M_2\ldots\ldots M_n)$

Step2: Each Member M_i will be assigned a P_i, a large prime number > K

Key generations:

Step 3: Take a prime number (or any number) $K < P_{i,}$ $\forall_{i.}$ That is:

$P_1 > K, P_2 > K, P_3 > K\ldots P_n > K$

Public Message Generation by Key Distribution Manager (KDM):

Step 4: Generate message $M = (P_1 * P_2 * \ldots . * P_n) + K$

Step 5: Multicast the above public Message M to all the members in the group

Derivation of Key (K) by each Member:

Step 6: Upon receiving the public message M, each member in the group will calculate the key in the following manner:

$K = M \bmod P_{i,}$ for all i.

Re-keying when new member join: Suppose if any new member wants to join the grid system:

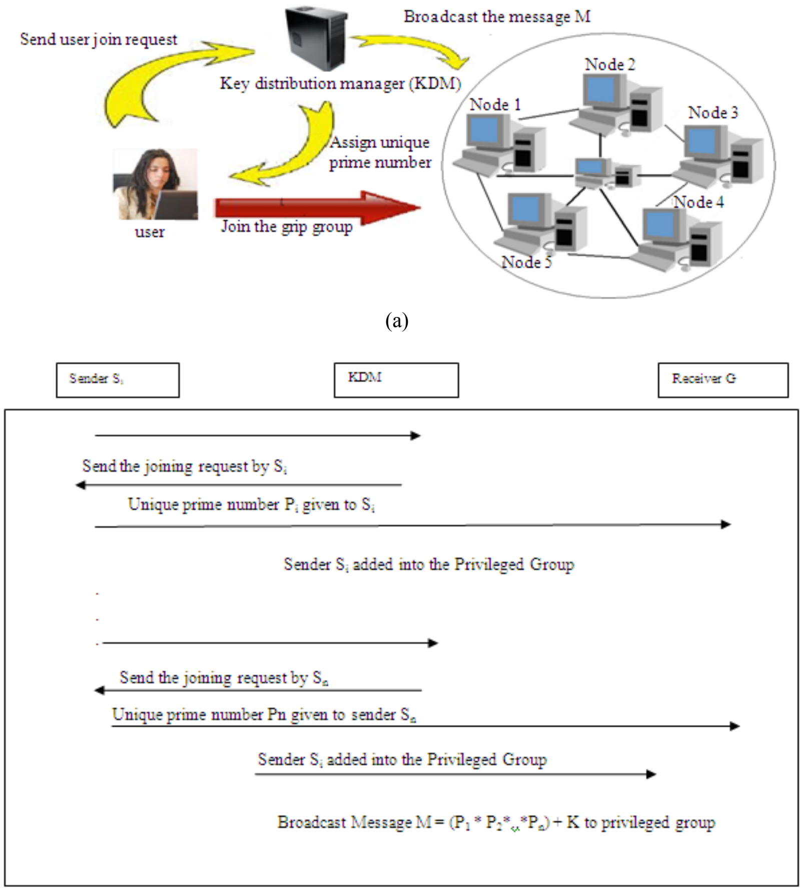
Step 1: The new member sends request to KDM (key distribution Manager) that it wishes to join the grid system. The KDM assigns new prime number $P_{n+1.,}$ where $K < P_{n+1}$

Step 2: Then the KDM generate the new public message $M' = (P_1 * P_2 * \ldots\ldots * P_n) * P_{n+1} + K$ and sends to the new member.

Step 3: The new members then calculate the Key by using from the message M'.
I.e. Remainder = $K = M' \bmod P_{n+1}$

Re-keying when existing member leaves:

Step 1: Suppose if any member j is willing to withdraw from the grid system the member should inform to the KDM or periodically check if there are ' n' members present in the grid system by sending M in case of no members have joined or relieved or M' in case of new members joined or left. Suppose if the KDM receives K alone by doing the above steps then no members have left.


Send user join request
Broadcast the message M
Key distribution manager (KDM)
Node 1
Node 2
Node 3
Node 4
Node 5
Assign unique prime number
user
Join the grip group
Sender S_i
KDM
Receiver G
Send the joining request by S_i
Unique prime number P_i given to S_i
Sender S_i added into the Privileged Group
Send the joining request by S_n
Unique prime number Pn given to sender S_n
Sender S_i added into the Privileged Group
Broadcast Message M = (P_1 * P_2*...*P_n) + K to privileged group

(a)

(b)

Fig. 1: General architecture for secure key distribution

Step 2: Then the KDM calculates the new public message as follows:

- Select or take a new K' (New prime number, where K' < P_i for all i)
- M''= $(P_1*P_2*P_3*....*P_{j-1})$ $(P_{j+1}*....P_n)$ + K' - (After leaving the j's prime number)

Step 3: Multicast the above public Message M'' to all the members in the group to maintain forward secrecy

Step 4: Upon receiving the public message M'' each member in the group will calculate the new key in the following manner

K = M'' mod P_i

The general architecture for secure key distribution is given in Fig. 1.

For simplicity, consider a grid with M=10 members. Let $Member_1$ has permanent secret identity, SID_1=55837, $Member_2$ has SID_2 =55603, $Member_3$ has SID $_3$=35353, $Member_4$ has SID $_4$=54709, $Member_5$ has SID_5=60779, $Member_6$ has SID_6=45953, $Member_7$ has SID_7=40847, $Member_8$ has SID_8=39461, $Member_9$ has SID_9=42709 and $Member_{10}$ has SID_{10}=58909 and key K= 229.By applying step4 of Public Message Generation by KDM, we generate the public message M=680145885919845305122185386484879441857328 25832 and multicast to all the ten members in the grid group. After receiving this public message, $member_1$ computes the key (K) by doing M % SID_1. i.e., K=680145885919845305122185386484879441857328 25832 % 55837. Similarly all the other members in the group calculate their keys by doing M % $SID_{i,}$ i=2, 3...10. It is just an illustrative example. We can take K (Key) sizes as 64,128, 512, 1024 bits and the value of SID (prime) could be 64, 128, 512 and 1024 bits.

Suppose there is a member P_k who has a SID_k=43651 and the above public message M. The member P_k cannot calculate the key. i.e., M mod P_k= 68014588591984530512218538648487944185732825832%43651=13699≠229≠K.

RESULTS

The performance of the algorithm for generating the message M for different group size is given in Fig. 2-7. In 2 and Fig. 5 show that our proposed certificate-free key distribution protocol takes less time for generating message for both small and large group sizes as well. Also 4 and Fig. 7 show the efficiency of our algorithm for small and large group sizes compared with dual-level key management for secure grid communication in dynamic and hierarchical groups. Similarly the efficiency of the algorithm for generating the key is given in Fig. 8-12. Figure 8 and 11 show that our proposed algorithm takes less time for generating key for both small and large group sizes. Also10 and Fig. 13 show the efficiency of our algorithm in generating the key for small and large group sizes compared with dual-level key management for secure grid communication in dynamic and hierarchical groups.

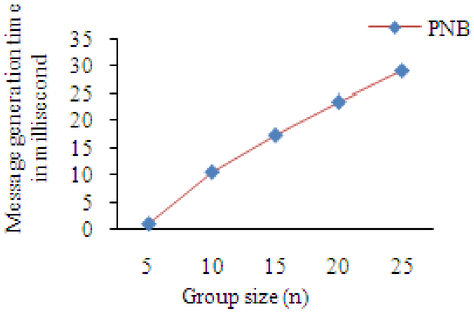


Fig. 2: Message Generation Using PNB

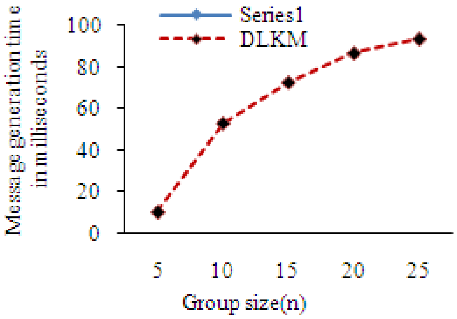


Fig. 3: Message generation using DLKM

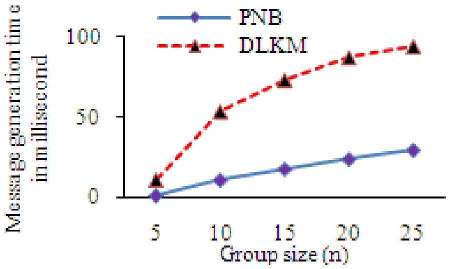


Fig. 4: Comparison of message generation

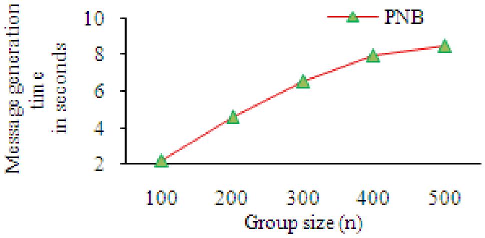


Fig. 5: Message generation for large group size:

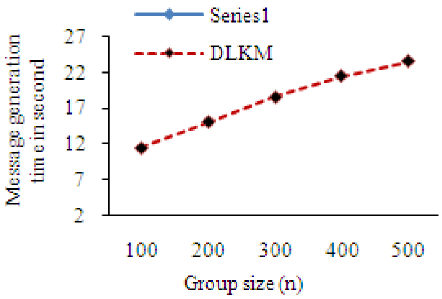


Fig. 6: Message generation for large group size:

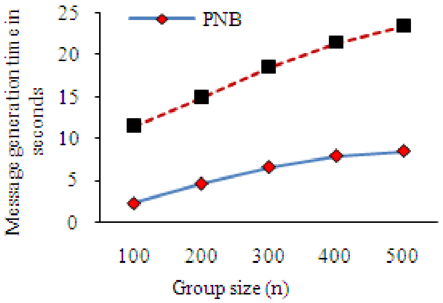


Fig. 7: Comparison of message generation:

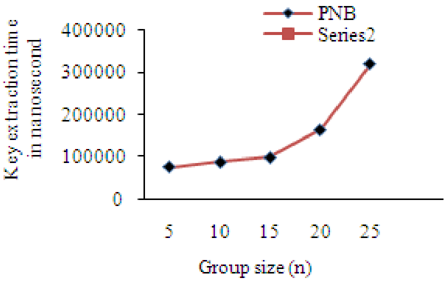


Fig. 8: Key extraction for small group size

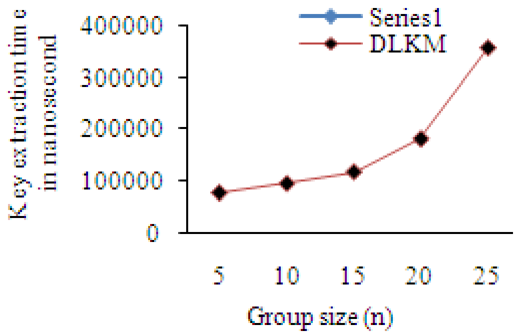


Fig. 9: Key extraction for small group size

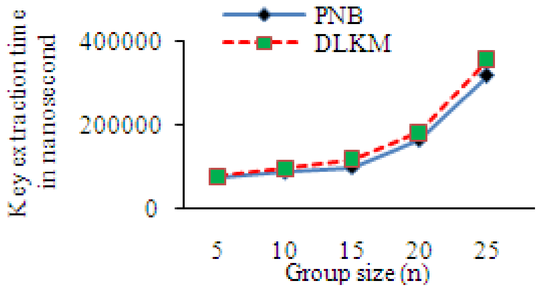


Fig. 10: Comparison of key extraction for small group

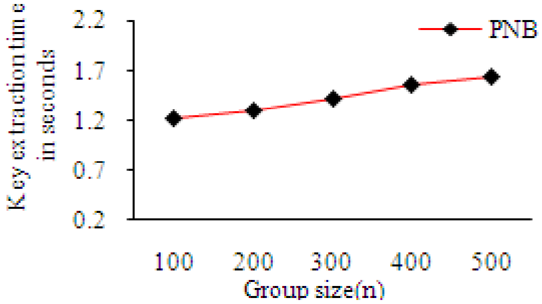


Fig. 11: Key extraction for large group

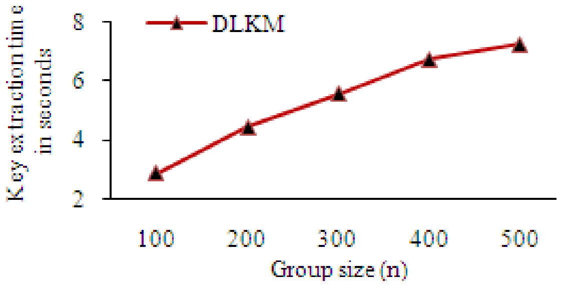


Fig. 12: Key extraction for large group

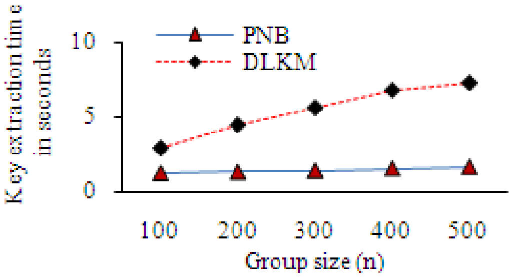


Fig. 13: Comparison of key extraction

DISCUSSION

Strength of the RSA algorithm relies on the fact that given M (the product of two large prime number), it is impossible to find the two factors which makeup M in polynomial time (It is NP-hard).In our algorithm, we have more complex message M, than what is used in RSA algorithm. Therefore, finding any of the prime numbers P_1, P_2, P_3,.....,P_n is NP-hard. Thus the key K is very safe and secure and prevents man-in-the middle and brute-force attacks. Similarly our algorithm computes new message and multicast it every time when a member joins/leave, to ensure both Forward Secrecy and Backward Secrecy.

CONCLUSION

We have proposed a simple yet an efficient certificate-free key computation protocol for secure group communication in dynamic grid environment. The experimental results show that our algorithm is efficient both in terms of message generation and key extraction In Future; we wish to implement our design in globus toolkit along with access control and measure the bandwidth utilization of these algorithms compared with dual-level key management for secure grid communication in dynamic and hierarchical groups.

REFERENCES

Amir, M., M. Jalal, A. Nasiri, B. Bahmani and M. Sadeghizadeh *et al*., 2008. DHA-KD: Dynamic hierarchical agent basedkey distribution in group communication. Proceedings of the IEEE 9th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, Aug. 06-08, IEEE Computer Society, Phuket, pp: 301-306. DOI: 10.1109/SNPD.2008.23

Hongweia, L., S. Shixina and Y. Haomiaoa 2008. Identity-based authentication protocol for grid. Syst. Eng. Elect., 19 860-865. DOI: 10.1016/S1004- 4132(08)60164-4

Ingle, R and G. Sivakumar, 2010. EGSI: TGKA based security architecture for group communication in grid. Proceedings of the 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, May 17-20, IEEE Computer Society, Australia, pp: 34-42. DOI: 10.1109/CCGRID.2010.28

Li, Y, H, Jin, Z, Han and S. Liu, 2009. A Secure mechanism of group communication for pervasive grid. Int. J. Ad Hoc Ubiquitous Comput., 4: 344-353. DOI: 10.1504/IJAHUC.2009.028662

Li1, Y., X. Xu, J. Wan, H. Jin and Z. Han, 2008. Aeolus: Reconcilable key management mechanism for secure group Communication in grid. Proceedings of the IEEE Asia-Pacific Services Computing Conferences (APSCC), Dec. 9-12, IEEE Computer Society, Yilan, pp: 1-7. DOI: 10.1109/APSCC.2008.227

Li1, Y., X. Xu, J. Wan, H. Jin and Z. Han, 2008. An authenticated encryption mechanism for secure group communication in grid. Proceedings of the International Conference on Internet Computing in Science and Engineering, Jan. 28-29, USA., pp: 298-05. DOI: 10.1109/ICICSE.2008.80

Park, H., W.S. Yi and Gang S. Lee 2010. Simple ID-based key distribution scheme. Proceedings of the 5th International Conference on Internet and Web Applications and Services (ICIW), May 09-15, IEEE Computer Society, Spain, pp: 369-373. DOI: 10.1109/ICIW.2010.61

Purusothaman, T., M.K. Balachandar and N. Arunkumar, 2010. An effective key computation protocol for secure group communication in heterogeneous networks. IJCSNS Int. J. Comput. Sci. Network Sec., 10: 313-319. http://paper.ijcsns.org/07_book/201002/20100247.pdf

Sudha, S., A. Samsudin and M.A. Alia, 2009. Group re-keying protocol based on modular polynomial arithmetic over Galois field GF (2n). Am. J. Applied Sci., 6: 1714-1717. DOI: 10.3844/ajassp.2009.1714.1717

Valli,V., D. Kumari, V. NagaRaju, K. Soumy and KVSVN Raju, 2010. Secure group key distribution using hybrid cryptosystem. Proceedings of the 2nd International Conference on Machine Learning and Computing, IEEE Computer Society, Washington, pp: 188-192. DOI: 10.1109/ICMLC.2010.41

Xukai, Z., Y. S. Dai and Xiang Rana, 2007. Dual- level key management for secure grid communication in dynamic and hierarchical groups. Future Generation Comput. Syst., 23: 776-786. DOI: 10.1016/j.future.2006.12.004

Zhenga, Y., H.Y. Wanga and R.C. Wang 2008. Grid authentication from identity-based cryptography without random oracles. J. China Univ. Posts Telecommun., 15: 55-59. DOI: 10.1109/CSSE.2008.1281