EAB-Euclidian Algorithm Based Key Computation Protocol for Secure Group Communication in Dynamic Grid Environment

Dr.M.Venkatesulu
Director, Senior Professor
Department of Computer Applications
Kalasalingam University, India
venkatesulu@kalasalingam.ac.in

Mr.K.Kartheeban
Selection Grade Lecturer
Department of Computer Applications
Kalasalingam University, India
k.kartheeban@klu.ac.in

Abstract

Grid Computing is mainly concerned with coordinated way of sharing diverse resources that are available in distributed "Virtual Organizations". A prominent feature of grid computing is the collaboration of multiple entities to perform collaborative tasks that rely on two important functions such as communication and resource sharing. 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. This paper proposes a simple and yet an efficient key computation and management protocols in dynamic Grid Environment based on Euclidian Algorithm (EAB).

Keywords*: Grid computing, Secure Group Communication.*

1. Introduction

The grid computing paradigm ([1],[2]) is concerned with sharing and coordinated use of diverse resources in distributed virtual organizations[VO] [7].Since the grid computing is heterogeneous, distributed and dynamic in nature, it manages resources and services distributed across multiple control domains. One of the most important considerations issues in grid computing is security. Since grid computing is internet-based and basically the network and internet are not security oriented by design, there could be various intruders constantly obtaining security holes existing in hardware, software, processes and system to perform various attacks. All the fundamental threats and attacks in network and internet are also applicable in grid computing. Moreover grid computing systems are group oriented; including a large number of users and shared resources and so the threats and attacks in grid systems may become more serious. Therefore providing security in this dynamic environment is much more important but very difficult. 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, or has common rules for resource sharing [22].Security in computational grids consists of authentication, authorization, non-repudiation, integrity, confidentiality and auditing. Confidentiality of information in a VO should also be ensured [7] As a result, providing centralized authentication and multiple-site co-

authentication is difficult to implement due to the distributed, heterogeneous and dynamic features of grid computing systems. The main aim of this paper is to develop time and bandwidth efficient key computation protocol for secure group communication in dynamic grid environment

The rest of this paper is organized as follows: In Section 2, a mechanism for group key management in grid computing is presented. In section 3, related work is discussed. In section 4, our approach for secure and efficient key computation protocol is proposed. The corresponding algorithms are analyzed with sample examples. In section 5, we present security analysis. Finally, in Section 6 we draw conclusion and propose direction for future research work.

2. Group Key Management Protocol

Some of the important applications like audio and video conferencing, pay-per-view, interactive chats groups and multi-user games are based on group communication mechanism. In this group communications several members participate and multicast communication is an efficient form of information sharing and distribution. But communication among members in the group should take into consideration factors like confidentiality, data integrity; authentication and access control. To achieve these, common group key or secret key must be calculated and distributed to all the members of a particular group. Since the group members in the heterogeneous network like grid is dynamic in nature, members can join and leave the group at any time. Managing the group key efficiently for large and dynamically changing group is a difficult problem. In order to ensure forward and backward secrecy the group key must be changed whenever member leaves or joins the group. Figure.1 shows Taxonomy of Group Key Management Protocols. Below we discuss three major approaches to group key management.

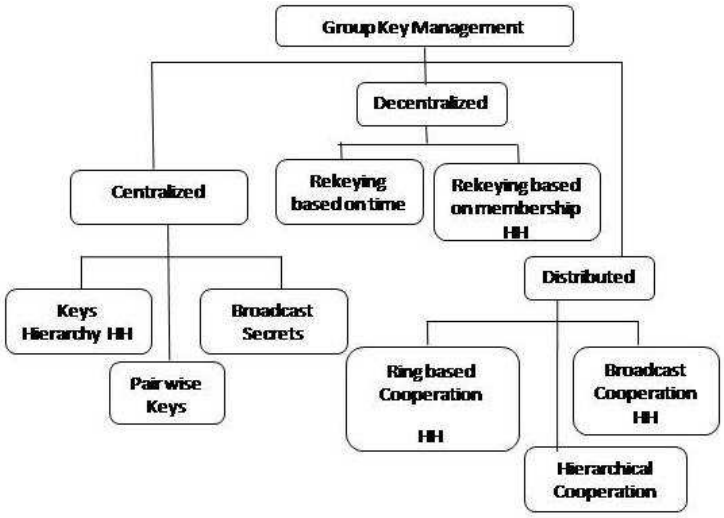


Figure 1. Taxonomy of Group Key

2.1. Centralized Group Key Management

In this type of key management, a single entity is employed for controlling the whole group. Hence a centralized key management seeks to minimize storage requirements, computational power on both client and server sides, and bandwidth utilization. But the major problem of this approach is a single point of failure.

2.2 Distributed Key Management

In distributed key management, there is no explicit KDC, and members themselves do the generation of the key. The members need not depend on third party. All members can perform access control and the generation of key is contributory, meaning that all members contribute some information to generate the group key. So the security level has been raised but this method is suitable for small groups only. For large groups collecting the contribution from every user is tedious and time consuming, and due to this reason scalability criterion is not fulfilled.

2.3 Decentralized Key Management

In a decentralized architecture, the management of a large group is divided among subgroup managers, there by trying to minimize the problem of concentrating the work in a single place. The Protocols used in Decentralized Key Management are SMKD, IGKMP and Hydra etc...[1], [3].

3. Related work

Security in computational grids consists of authentication, authorization, non-repudiation, integrity, confidentiality and auditing. To achieve security in grid some technologies have been already used to build the 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. Authorization allows a specific permission for a particular user on a specified resource. The necessity for secure communication between grid entities has motivated the development of the Grid Security Infrastructure (GSI).GSI provides integrity, protection, confidentiality and authentication for sensitive information transferred over the network in addition to the facilities to securely traverse the distinct organizations that are part of collaboration [2]. Authentication is done by exchanging proxy credentials and authorization by mapping to a grid map file. Grid technologies have adopted the use of X.509 identity certificates to support user authentication. GSI is built on top of the Transport Layer Security (TLS) protocol. Both TLS and GSI operate at the transport layer. They require an ordered reliable transport connection, so typically they are implemented over Transmission Control Protocol (TCP). This approach is not suitable for web service-based technologies on the grid. In [3] Xukai Zoua, Yuan-Shun Dai and Xiang Rana have proposed an elegant Dual-Level Key Management (DLKM) mechanism using Access Control Polynomial (ACP) and one-way functions. The first level provided flexible and secure group communication whereas the second level offered hierarchical access control. Li Hongweia et al. [4] have proposed an identity-based authentication protocol for grid on the basis of the identity-based architecture for grid (IBAG) and corresponding encryption and signature schemes. Being certificate-free, the authentication protocol aligned well with the demands of grid computing. Yan Zhenga et al [5] use identity-based signature (IBS) scheme for grid authentication. Hai-yan Wanga. C and Ru-chuan Wanga [6] have proposed a grid authentication mechanism,

which is based on combined public key (CPK) employing elliptic curve cryptography (ECC).Confidentiality of information in a VO should also be ensured [7].

In [11] S.Jabeenbegum, T.Purusothaman et al proposed cluster based hierarchical key distribution protocol for secure group communication. This approach uses prime number addition for member joining and leaving. In [8] Li proposed a 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 rates that the group members join and leave. A scalable service scheme for secure group communication using digital signatures to provide integrity and source authentication is proposed by Li [9]. In this approach, Huffman binary tree is used to distribute keys in VO and complete binary tree is used to manage keys in administrative domain. In [10] Li et al. proposed an authenticated encryption mechanism for group communication in terms of the basic theories of threshold signature and basic characteristics of group communication in grid. In this mechanism, each member in the signing group can verify the identity of the signer, and the verifying group keeps only private key. M.AmirMoulavi, Jalal, A.Nasiri, BehnamBahmani et al. [12] 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. In [13] Shouzhi XU et al proposed minimum exact cover problem of leaf set and discusses its solution based on a-ary tree model. In this approach the efficiency and effectiveness of the group key distribution is achieved based on minimum exact cover. In [19] Rajesh Ingle 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.

4. Euclidian Algorithm Based Key Computation Protocol (EAB)

When a member or an organization is willing to join the grid, he/she can join the grid only by using the globus toolkit. During this joining process there are several certificates which 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 PSN_i (personal Security Number) for each member/node/machine M_i.During the registration process, the permanent personal security number can be embedded into the certificates issued to the member.

4.1. Group Key Formation Using EAB

For a group of users participating in a grid service, the Key Distribution Manager (KDM) will generate (a_i, b_i) pairs for each PSN_i using PSN_i .

Step 1:

Consider that there are is ‘n’ number of members in the grid (m_1, m2, m3...m_n)

Step 2:

Assign a personal security number PSN_i (prime number P_i) to each member when

they request to join in the group. The size of the prime can be (512 bits, 1024 bits, 2048 bits and etc)

Step 3:

The KDM selects a random group key K > PSN_i for all i for group G and computes the message (a_i, b_i) pairs in the following manner:

$$a_i = K / PSN_i \quad (1)$$

$$b_i = K \bmod PSN_i \quad (2)$$

Finally the KDM publicizes (a_i , b_i).From this public information, any group member m_i can get the key by computing

$$K = a_i * PSN_i + b_i \quad (3)$$

It is assumed that the member m_i would recognize the pair (a_i, b_i) meant for it.

No member M_k other than m_i can get the hidden key K using (a_i , b_i) .This key management mechanism guarantees that only a member whose PSN_i included in the calculation of (a_i , b_i) pairs can drive the key from (3).

Using this scheme, dynamic groups can be easily managed for joining and leaving member. If a new member U_r needs to be added, the KDM generates a new PSN_i and assign it to U_r. Then the KDM generate (a_i , b_i) pairs by using the eq. (1) and (2). After receiving the (a_i , b_i) pairs,U_r can use the PSN_i to derive the key K from Eq.(3).Only in case of a member leaves the group the common key K need to be changed.

4.2. Illustrative Examples

Let there be 4 members in the group.$Member_1$ has personal security number PSN_1=12, Member2 has PSN_2=17, Member3 has PSN_3=19 and $Member_4$ has PSN_4=7.The group secret key K should be distributed to all the above four members. Suppose K=26.By Eq.(1) and (2),the following pairs will be generated using the each members PSN and K as follows.

Pair for $member_1$ $a_1 = K / PSN_1$ and

$b_1 = K \bmod PSN_1$. Hence (a_i, b_i) = (2, 2)

Similarly, for other members, the pair (a_2, b_2) = (1, 9), (a_3, b_3) = (1, 7) and (a_4, $b_{4)}$ = (3, 5)

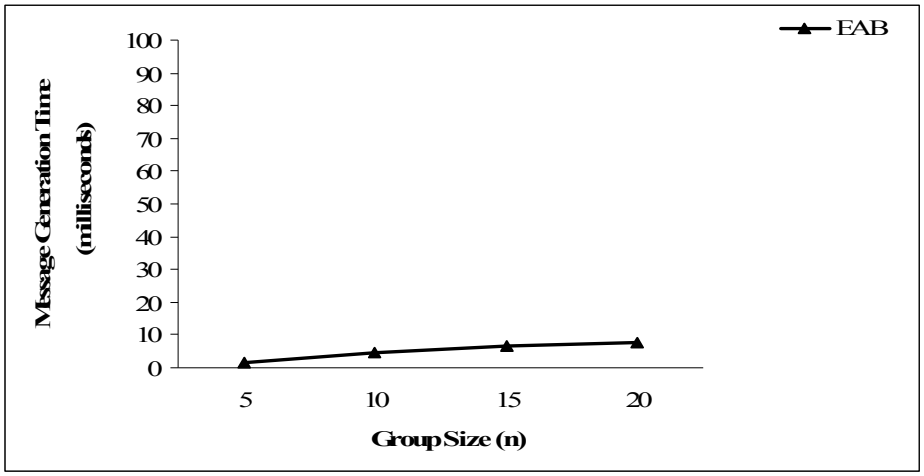
These messages are sending to the group members. After receiving these messages member1 computes the key by using its pair as follows: $K_1 = (a_1 * PSN_1) + b_1 = (2 * 12) + 2 = 24+ 2=26=K$.$Member_2$ obtains K= 1 * 17 + 9= 26.Similarly $Member_3$ obtains K= 1 * 19 + 7= 26 and $Member_4$ obtains 26 too.

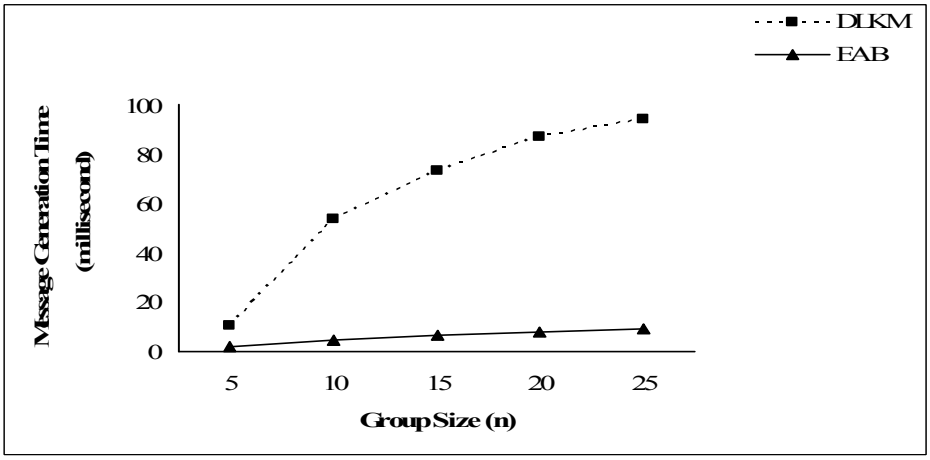
The above is just an illustrative example. In real case implementation, the PSN will not be as small as 13,17 and 19 etc. We can take K (Key) sizes as 128, 512, 1024 bits and also the value of PSN (prime) could be 128,512 and 1024 bits.

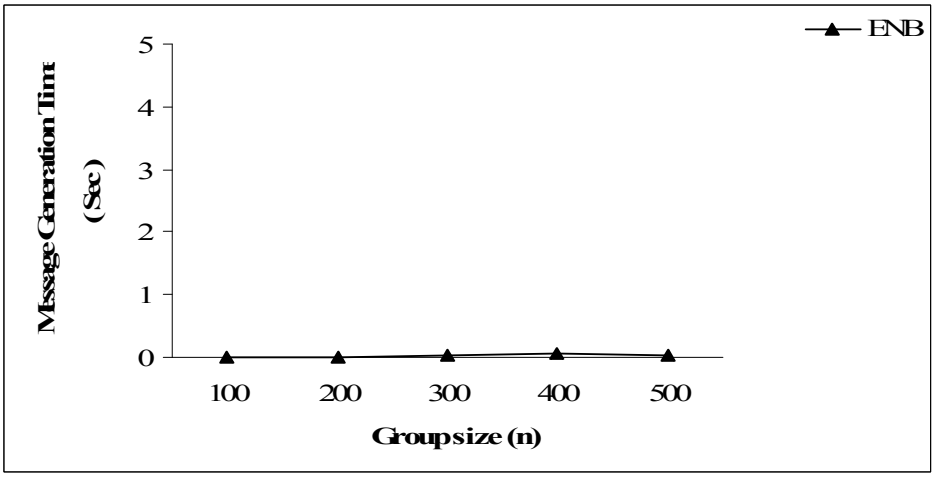
Suppose there is a member m_k who has a PSN_k=43 and obtains any one of the pairs (a_i, bi). Assume that the member m_k gets the pair (1, 9). But the key K can not be generated correctly .Here we have 26= K≠ 1 *43 + 9 =52.Similarly 26=K≠ (2 * 43) + 2= 88 and so on.

Generating pairs of numbers from the personal security number (PSN) and K is very simple and effective and it takes less time. The performance of this algorithm for generating the pairs for various group sizes is given in Figure 2 and Figure 3. Figure 2.shows the efficiency of the algorithm for generating message for different group sizes. Similarly Figure 3.shows the efficiency of the algorithm for key extraction for different group sizes .The

proposed algorithm is compared with the polynomial algorithm (DLKM) for secure group communication and the results are given in Figures 2 and 3.







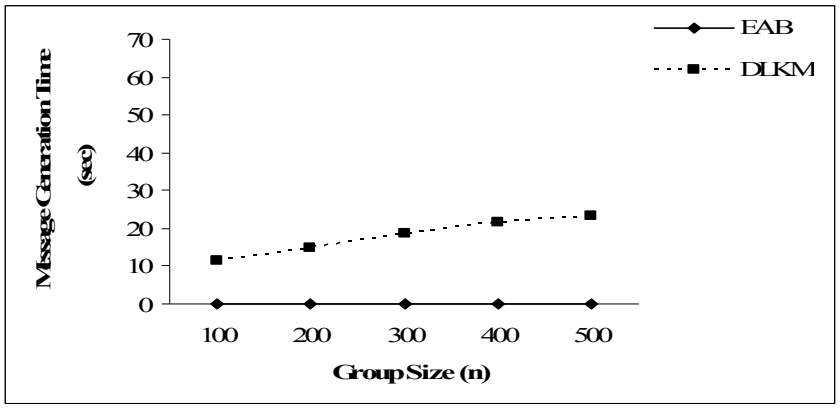
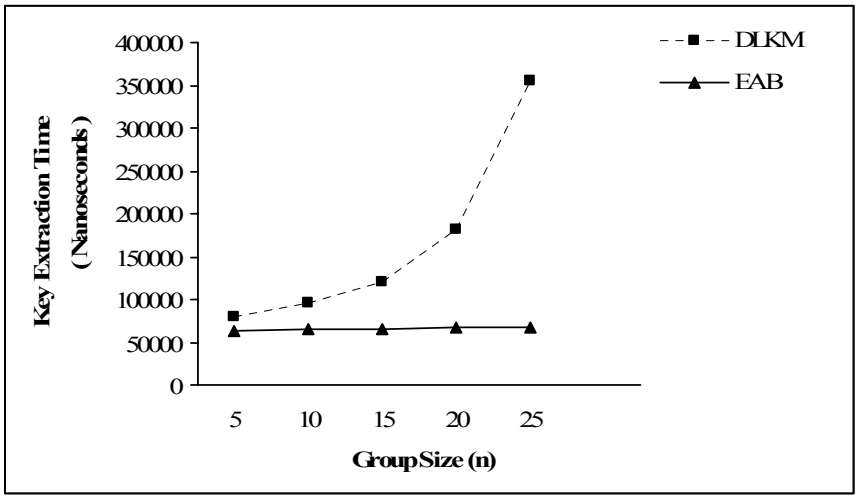


Figure 2. Group size vs. Message generation time

The processing time for key extraction with different group sizes for the polynomial algorithm and the proposed Euclidian Algorithm Based (EAB) are shown below and EAB algorithm performs better.



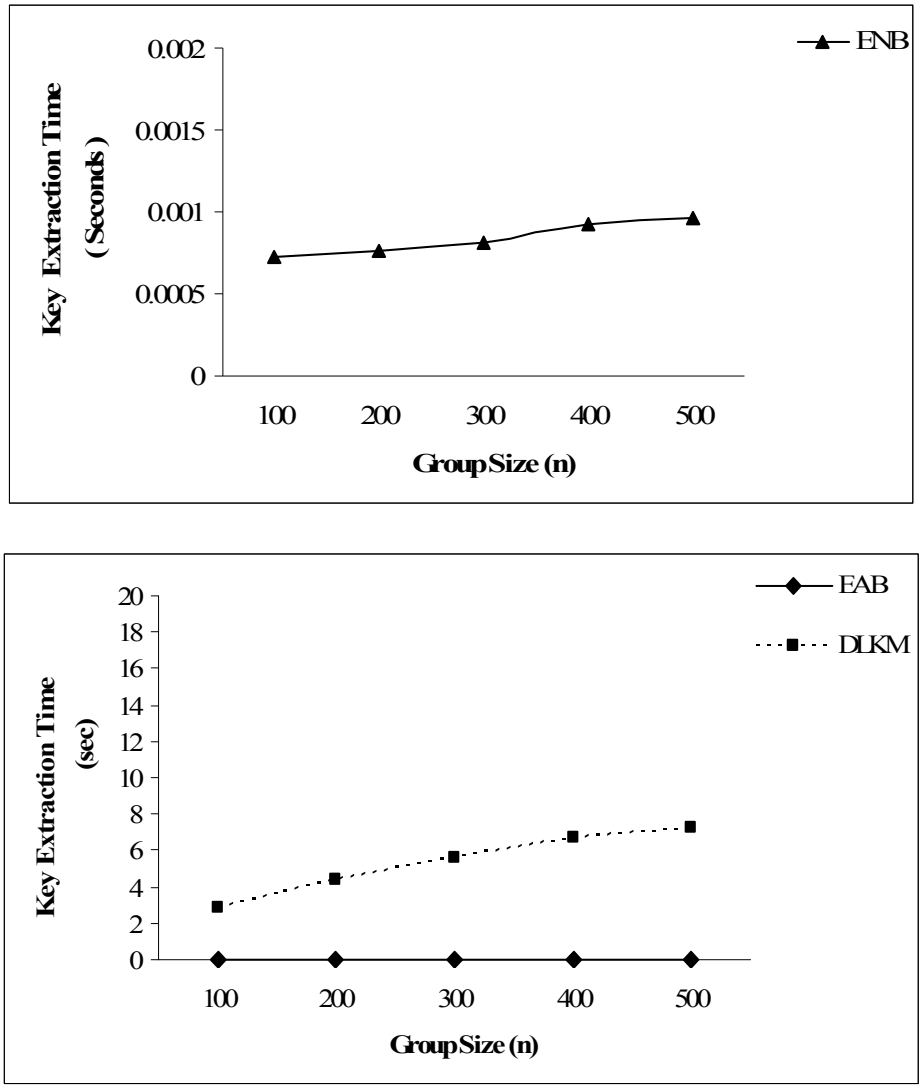


Figure 3. Group size vs. Key extraction time

5. Security Analysis

Given K and P, it is easy to compute

$$a = K / P \text{ and } b = K \bmod P.$$

But given a and b it is very difficult to compute K, in polynomial time, without knowing P such that K = aP + b, and it is NP hard for large size of K.Even if several pairs (a_i, b_i) are known, it is very difficult to compute K, unless the corresponding pi's are known.

Suppose,

$$K = a_1P_1 + b_1 \quad (P_1 \text{ not known}) \tag{1}$$

$$K = a_2P_2 + b_2 \quad (P_2 \text{ not known}) \tag{2}$$

$$K = a_3P_3 + b_3 \quad (P_3 \text{ not known}) \tag{3}$$

$$K = a_4P_4 + b_4 \qquad (P_4 \text{ not known}) \tag{4}$$

From the first of two equations, we get

$$a_1P_1 + b_1 = a_2P_2 + b_2 \qquad a_1P_1 - a_2P_2 = b_2 - b_1 \quad (\text{say } b_2 > b_1)$$

$$a_1P_1 - a_2(P_1 + r_1) = C_1 \quad (b_2 - b_1 = C_1,\ P_2 = P_1 + r_1)$$

$$(a_1 - a_2)P_1 - a_2r_1 = C_1 \tag{5}$$

Similarly from 1 and 3, we get

$$(a_1 - a_3)P_1 - a_3r_2 = C_2 \tag{6}$$

From 2 and 3, we get

$$(a_2 - a_3)P_2 - a_3r_3 = C_3$$

$$(a_2 - a_3)(P_1 + r_1) - a_3r_3 = C_3$$

$$(a_2 - a_3)P_1 + (a_2 - a_3)r_1 - a_3r_3 = C_3 \tag{7}$$

Thus, there only 3 equations (5 – 7) to determine 4 unknowns (r_1, r_2, r_3 and P_1), Therefore one of the values r_1 or r_2 or r_3 or P_1 will be left arbitrary, hence the value of K can not be determined correctly.

6. Conclusion

We have designed a simple and efficient key computation protocol for secure group communication in dynamic grid environment. Its performance is compared with DLKM (polynomial algorithm) and our algorithm performs better both on key message generation and key extraction. In future, we wish to extend the results to the hierarchical access control in dynamic grid environment.

References

[1] I. Foster, Carl. Kesselman, J.M. Nick, and S. Tuecke,"Grid Services for Distributed Systems Integration", IEEE Computer Society, Volume 35 Issue 6, June 2002, pp. 37- 46.
[2] Foster, I., C. Kesselman, In the Grid: Blueprint for a New Computing Infrastructure, Morgan Kaufmann, San Francisco, 1999.
[3] Xukai Zoua, Yuan-Shun Dai and Xiang Rana, "Dual-Level Key Management for secure grid Communication in dynamic and hierarchical groups", Future Generation Computer Systems, Science Direct, 2007 Volume 23, Issue 6, July, pp.776-786.
[4] Li Hongweia, Sun Shixina and Yang Haomiaoa, "Identity-based authentication protocol for grid", Journal of Systems Engineering and Electronics, Elsevier, Volume 19, Issue 4, August 2008, pp. 860 - 865.
[5] 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, Elsevier, Volume 15, Issue 4, December 2008, pp. 55 - 59.
[6] C. Hai-yan Wanga and Ru-chuan Wanga,"CPK-based grid authentication: a step forward", The Journal of China Universities of Posts and Telecommunications, Elsevier, Volume 14, Issue 1, March 2007, pp .26 - 31.
[7] V. Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman and S.Tuecke, "Security for Grid Services", in proceedings of the 12th IEEE International Symposium on High Performance Distributed Computing, 2003, pp. 48- 57.
[8] Y. Li, X. Xu, J. Wan, H. Jin, and Z. Han, (2008) 'Aeolus: reconcilable key management mechanism for secure group communication in grid', IEEE Asia-Pacific Services Computing Conference, 2008, pp. 1 – 7.

[9] Y. Li, H. Jin, D. Zou, S. Liu, and Z. Han, (2007) 'A scalable service scheme for secure group communication in grid', 31st Annual International Computer Software and Applications Conference (COMPSAC 2007), 2007, pp. 31 - 38.
[10] Y. Li, H. Jin, D. Zou, S. Liu, and Z. Han, 'An authenticated encryption mechanism for secure group communication in grid', International Conference on Internet Computing in Science and Engineering, 2008, pp. 298-305.
[11] S. Jabeenbegum, T. Purusothaman, M. Karhti, N. Balachandran, and N. Arunkumar, "An Effective Key Computation Protocol for Secure Group Communication in Heterogeneous Networks", International Journal of Computer Science and Network Security, February 2010, pp. 313-319.
[12] M.A. Moulavi, J.A. Nasiri, B. Bahmani, M. Sadeghizadeh, and M. Naghibzadeh,"DHA-KD:Dynamic Hierarchical Agent Based Key Distribution in Group Communication", IEEE Ninth ACIS international Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Phuket, 2008, pp. 301 – 306.
[13] Shouzhi XU, Tingyao Jiang, Alin Zhong, Wangmin Yang, Lili Zhang, and Qiaoli Liu, "A-ary Tree-based Minimum Exact Cover of Leaf Set for Secure Group Communication in Grids", Sixth International Conference on Grid and Cooperative Computing (GCC 2007), 2007, pp. 11 - 18.
[14] Haeryong Park, W.S. Yi, and Gang Shin Lee," Simple ID-Based Key Distribution Scheme", Fifth International Conference on Internet and web Applications and Services, 2010, pp. 369 - 373.
[15] V.Valli Kumari, D.V. NagaRaju, K. Soumya, and K.V.S.V.N. Raju,"Secure Group Key Distribution Using Hybrid Cryptosysytem", Second International Conference on Machine Learning and Computing,2010,pp.188-192.
[16] S. Eskeland and V. Oleshechuk, "Secure Group Communication using fractional public keys", International Conference on Availability, Reliability and security, 2010, pp. 254 – 257.
[17] R. Aparna, B.B. Amberker, DivyaPola, and Pranjal Bathia,"Secure Group Communication using Binomial trees", IEEE 3rd International Symposium on Advanced Networks and Telecommunication Systems (ANTS), 2009, pp. 1 – 3.
[18] Yunfa Li, Hai Jin,Deqing Zou, Sanmin Liu and Zongfen Han," A secure mechanism of group communication for pervasive grid", International Journal of Ad Hoc and Ubiquitous Computing, September 2009, pp. 344-353.
[19] Rajesh Ingle, and G. Sivakumar, "EGSI: TGKA Based Security Architecture for Group Communication in Grid", 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, 2010, pp. 34 - 42.
[20] I. Foster, C. Kesselman, and S. Tuecke, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations", International Journal of High Performance Computing Applications", ACM Digital Library, August 2001, pp. 200 - 222.

Authors

M. VENKATESULU received his post graduate degree in Mathematics from Sri Venkateswara University, Tirupati, India in 1975 and Ph.D. in Mathematics from Indian Institute Technology, Kanpur in 1979, He worked as a faculty at Shri Sathya Sai University, Prashanthinilayam, India between 1983 and 2002. He worked as a consultant for Satyam Computers, Hyderabad, India for a short period. He was visiting professor at the University of Missouri, Kansas City, USA between August 2006 and May 2007. Currently, he is a senior professor and Head of the Department of Computer Applications at Kalasalingam University, Krishnankoil, Srivilliputtur(via), Tamil Nadu, India. His areas of interests include differential equations, image processing, cryptography and bioinformatics and grid computing

K. KARTHEEBAN, He is a Selection Grade Lecturer in Department of Computer Applications, Kalasalingam University, Krishnankoil, and Tamilnadu, India. He received his B.Sc in Mathematics and Master's degree in Computer Applications from Madurai Kamaraj University. He also obtained his Master of Engineering in Computer Science from Anna University, Chennai. Currently he is pursing his doctoral degree in the field of security in grid computing.