International Journal on Recent Researches In Science, Engineering & Technology

A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy.

It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in DIIF and SJIF.

Research Paper

Available online at: www.jrrset.com

Chief Editors 1 : Dr. M.Narayana Rao, Ph.D., Rtd. Professor, NIT, Trichy.
(Engg.&Technology division)
2 : Dr. N.Sandyarani, Ph.D., Professor,
Chennai based Engg.College, (Science division)

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

Volume 2, Issue 4,
April 2014

DIIF IF :1.46
SJIF IF: 1.329

A Secure Group Communication Using Non-Interactive Key Computation

S . Kalaselvi

Abstract : Literature reported that broadcast encryption deals with broadcasting an encrypted message , so that only a set users termed privileged can decrypt it . These privileged set can be formed by selecting the users among the users within the group . To make sure that the data is available only to privileged users in the group of secret key is used which is known only to members of privileged set at any instant of time . Using secret key sender encrypt the data and sends , receiver in turn decrypts it . This privileged set is known as secure group , communication within the set as secure group communication . Since the secure group is dynamic in nature members in the group may change over time, i,e., new members may join the ground and existing members may leave the group . As group membership changes key must be changed and redistributed securely to all authorized users . This type of communication provides only confidentiality . Providing authentication in addition to confidentiality is an important issue in secure group communication . A protocol is designed for against multiparty authentication scheme which allows all the users in the system to send the receive message simultaneously . Since all the group members in the system to send the receive message, the sender of the message must be able to indicate his identity and the receiver must be able to verify the authenticity of the message. To verify the authenticity the key is formed by non-interactively with the help of information obtained by key distribution centre (KDC). This scheme is secure against colliding malicious parties numbering more than k(threshold).This scheme provides authenticity by using a part of information keys which is used for secret key

computation , thus without increasing the storage at the user.