Secure Group Key Sharing Protocols and Cloud System

Vaishali Ravindra Thakare
VIT University, India

John Singh K
VIT University, India

INTRODUCTION

Secure group communication is an important research issue in the field of cryptography and network security, because group applications like online chatting programs, video conferencing, distributed database, online games etc. is expanding rapidly. Group key agreement protocols allow that all the members agree on the same group key, for secure group communication, and the basic security criteria must be hold. Many group key agreement protocols have been established for secure group communication.

Since the group generation processes takes many modular exponentiations and long time in generation of group key. For achieving higher security, group key protocol should be dynamic, means it should change for each new join or leave member, so that new member have not any knowledge about prior information. Therefore group key management protocol focusing on the group key generation efficiently. The authors have identified the research gaps in the existing protocols and these are communication, computation overhead while generating and sharing digital envelopes and security issues while sharing group key with encryption algorithms. These research problems in existing framework motivate authors to focus on security and efficiency of the system. Many practical systems have been proposed (Liu et al., 2014a, 2015; Pan et al., 2011; Sanchez-Artigas, 2013; Li et al., 2015) of which the most familiar one is the TGDH key distribution system. After analyzing the demand for sharing data with multiple users in groups by reducing computational complexity and for achieving productive benefits, an efficient solution is proposed in this paper.

Modular exponentiation is very expensive in computation of group key. The number of exponentiations for membership depends on group size as when the group size increased the number of exponents will also increase. Tree Based Group Diffie Hellman (TGDH) (Kim et. al., 2004) uses the concept of Diffie-Hellman key exchange with logical tree structure to achieve efficiency. The efficiency of TGDH is O (log2n), where n is the group size. However, some extra overhead occurred in maintaining a perfect key tree balance. Skinny tree has lower communication overhead, but it increases computation. Burmester–Desmedt (BD) distributes and minimizes computation by using more messages broadcast. All these protocols using similar security properties including group key independence. From the broad study it is found that, tree-based CGKA (Contributory Group Key Agreement) methods are more efficient since they reduce the complexity from O (n) to O (log n) while computing the new group key, where n is the group size. Consequently, this unit considers only the existing tree-based CGKA protocols.

DOI: 10.4018/978-1-5225-2255-3.ch145

BACKGROUND

Group key agreement protocols allow that all the members agree on the same group key, for secure group communication, and the basic security criteria must be hold. In 1994 Mike Burmester and Yvo Desmedt Proposed A Secure and Efficient Conference Key Distribution System (BD Protocol), In 2000 Group Diffie Hellman (GDH) was proposed by Steiner et.al., Skinny Tree (STR) Wong et al. 2000, ID-AGKA (Identity based authenticated group key agreement protocol) by K C Reddy and Divya Nalla in 2002, Kim et al. proposed TGDH (Tree Based Group Diffie Hellman) in 2004, In 2006 CCEGK was proposed by Szheng, Moreover in 2009 QGDH (Queue Based Group Diffie Hellman) by Hong S.

After understanding the real time issues in real time groupware applications like voice & video conferences, distributed computation over the insecure network.

(Zheng et al., 2007) Proposed a two round key agreement protocol for dynamic peer group (DPG). The protocol is proven secure against passive attack by using indistinguishable method. Moreover, both perfect forward secrecy (PFS) and key independence (KI) were achieved. Author's proposed protocol greatly reduces the computation complexity of each member, definite identification and time stamp are added to the protocol to effectively avoid replay attacks and it satisfies PFS, dynamic and it provides a session key for wireless group members due to which its messages are transmitted through broadcasting. Meanwhile, authors proved correctness, tolerance for passive attacks, secure against active adversaries in the random oracle model as the security and efficiency analysis of this protocol.

(Liu et al., 2013) Proposed a secure multi-owner data sharing scheme (Mona) for dynamic groups in cloud applications. The Mona aims to realize that a user can securely share the data with others via the un-trusted cloud servers, and efficiently support dynamic group interactions. In this scheme, a new user can directly decrypt data files without pre-contacting with data owners, and user revocation is achieved by revocation list without updating the secret keys of the remaining users.

(Xue & Hong., 2013) proposed a novel secure group sharing framework for public cloud and it can take the effective advantage of cloud help by taking care that no sensitive data should be exposed to cloud provider and an attacker. It combines proxy signature, enhanced TGDH-based binary tree, proxy re-encryption as a protocol, using which the authors have achieved the objective. In this scheme, authors used TGDH with binary tree to negotiate and update the group key pairs with the help of cloud servers

(Jaiswal & Tripathi., 2015) Proposed an alternative approach to group key agreement, i.e., a novel queue-based group key agreement protocol, which uses the concepts of elliptic curve cryptography to reduce unnecessary delays, considers member diversity with filtering out low performance members in group key generation processes. After analyzing many prior group key agreement protocols like TGDH, STR, BD, and QBDH, they provide better security. They take more computational overheads. So, authors have used elliptic curve cryptographic technique that removes exponentiation to reduce computational overheads, and hence the results are better than that of the other group key agreement protocols.

Figure 1 shows the tree structure of CGKA, the management of secure communication among groups of participants requires a set of secure and efficient operations some protocols are better in communication cost some are in computation of secure group key while some are having security issues. These all protocols fall under CGKA (Contributory Group Key Agreement) scheme. CGKA is further again Divided into two sub categories:

Tree Based-CGKA

STR (Skinny Tree)

The STR protocol is modified to provide dynamic group operations. The protocol has a relatively