Secure Group Message Transfer Stegosystem

Mahinder Pal Singh Bhatia, Department of Computer Engineering, Netaji Subhas Institute of Technology, New Delhi, India

Manjot Kaur Bhatia, Department of Computer Science, University of Delhi, New Delhi, India

Sunil Kumar Muttoo, Department of Computer Science, University of Delhi, New Delhi, India

ABSTRACT

Grid environment is a virtual organization with varied resources from different administrative domains; it raises the requirement of a secure and reliable protocol for secure communication among various users and servers. The protocol should guarantee that an attacker or an unidentified resource will not breach or forward the information. For secure communication among members of a grid group, an authenticated message transferring system should be implemented. The key objective of this system is to provide a secure transferring path between a sender and its authenticated group members. In recent times, many researchers have proposed various steganographic techniques for secure message communications. This paper proposes a new secure message broadcasting system to hide the messages in such a way that an attacker cannot sense the existence of messages. In the proposed system, the authors use steganography and image encryption to hide group keys and secret messages using group keys in images for secure message broadcasting. The proposed system can withstand against conspiracy attack, message modification attack and various other security attacks. Thus, the proposed system is secure and reliable for message broadcasting.

Keywords:
Grid Environment, Group Key, Secure Group Communication, Secure Inter Group Communication, Secure Message Broadcasting, Steganography

1. INTRODUCTION

Security is one of an important issue and essential requirement in grid environment. Grid allows users from multiple domains to work in groups by sharing information with each other. Secure group communication is applicable in various applications such as interactive simulations, multiparty military actions, government discussions on critical issues and real time information services. To secure communication among members of a group working on collaborative tasks, grid environment requires implementation of additional security mechanisms. Secure group communication in grid needs to guarantee confidentiality and validity of the message to confirm the receiver that message is forwarded by the authorized user.

DOI: 10.4018/IJISP.2015100103

The main objective of secure group message transferring system is to create a secure environment between the sender and the authorized receivers for sharing some information in a secure way. In the secure group message transferring protocol, the message communication among the sender and the receivers forming the group must be confidential. Thus, only the authorized group members can extract the message, and the unauthorized members cannot access any important information. This brings the need of secure communication protocol responsible for generating secure group key and providing authenticated secure message transferring between group members. To provide these security functions, secure communication protocol needs to generate a group key/session key for the group members based on their secret information.

Our Secure group message transferring stegosystem (SGMS) protocol is based on steganography and image encryption technique to mask secure messages in such a way that an attacker could not know that any message is being communicated in the group. This paper extends our previous work (Bhatia et al., 2013) and proposes a new secure group message transferring stegosystem that can guard the group communication in grid environment against various security attacks, such as conspiracy attack, message modification attack. As a result, the proposed stegosystem not only has advantages of the secret message transferring system, but also is more protected and realistic in comparison to already proposed message transferring system. The remainder of this paper is organized as follows: Section 2 discusses group communication protocols already proposed by various researchers. Section 3 presents brief outline of our already proposed secure group communication protocol. The newly proposed stegosystem is presented in Section 4, while Sections 5 discusses its security features. Section 6 presents the simulation and experimental results and performance, respectively. Finally, Section 7 concludes the paper.

2. RELATED WORK

Researchers have proposed different protocols for secure group communication between grid entities. Researchers used either centralized or distributed group key management protocols for secure group communication. Most of the researchers have used encryption schemes/algorithms to provide secure group communication among various group members. Dual Level Key Management protocol (DLKM) that uses access Control Polynomial (ACP) and one-way functions to provide flexibility, security and hierarchical access control was proposed by Zoua (Zoua et al., 2007). Researchers used encryptions to update the group key for forward and backward secrecy. Li (Li et al., 2007) proposed a scalable service scheme using digital signatures and used Huffman binary tree to provide security and integrity. In this approach, Huffman binary tree is used to distribute and manage keys in VO and complete binary tree is used to manage keys in administrative domain. Park, (Park et al., 2010) have proposed an ID-based key distribution scheme that uses cryptographic algorithms to offer security and offer scalability. Li (Li et al., 2008) have proposed an authenticated encryption mechanism for group communication with basic characteristics of group communication in grid in terms of the basic theory of threshold signature. Several researchers have proposed various systems (Liao, 2007; Huang, 2010; Liaw, 1999) based upon different cryptographic techniques. Most of these systems encrypt the messages and send it to the members of its group. Liaw (Liaw, 1999) proposed a secure broadcasting cryptosystem based on the RSA and symmetric encryption algorithms, which allows addition of new users into the active groups. Tseng and Jan (Tseng and Jan, 2001) pointed out that Liaw's broadcasting system is not secure against conspiracy attack; an intruder can break its security and can obtain the master secret key. To overcome this problem, Tseng and Jan proposed a modified broadcasting cryptosystem. Masque and Peinado (Masque and Peinado, 2006) pointed out some

Related Content

A Rule-Based and Game-Theoretic Approach to Online Credit Card Fraud Detection

Vishal Vatsa, Shamik Sural and A. K. Majumdar (2007). *International Journal of Information Security and Privacy (pp. 26-46).*
www.igi-global.com/article/rule-based-game-theoretic-approach/2465?camid=4v1a

Uncovering Limitations of E01 Self-Verifying Files

Jan Krasniewicz and Sharon A. Cox (2019). *Advanced Methodologies and Technologies in System Security, Information Privacy, and Forensics (pp. 34-46).*
www.igi-global.com/chapter/uncovering-limitations-of-e01-self-verifying-files/213636?camid=4v1a