Chapter 109
A Novel Trust Model for Secure Group Communication in Distributed Computing

Naresh Ramu
SRM Institute of Science and Technology, India

Vijayakumar Pandi
University College of Engineering, Tindivanam, India

Jegatha Deborah Lazarus
University College of Engineering, Tindivanam, India

Sivakumar Radhakrishnan
University College of Engineering, Tindivanam, India

ABSTRACT

Distributed networks are networks in which each node can act as a server or client and hence any node can provide service to any other node. In such a scenario, establishing a trust model between the service providing user and the service utilizing user is a challenging task. At present, only a few approaches are available in the past literature to provide this facility. Moreover, the existing approaches do not provide high trust accuracy. Therefore,a novel efficient trust model has been proposed in this article to support the secure dynamic group communication in distributed networks. The main advantage of the proposed work is that it provides higher trust accuracy. Moreover, the proposed work takes less memory for maintaining the trust values and increases the packet delivery ratio in comparison with other existing works which are in the literature.

DOI: 10.4018/978-1-7998-5339-8.ch109

INTRODUCTION

In the recent years, rapid development of the distributed computing has numerous realtime applications, which incorporates a number of relative technologies such as cloud computing, utility computing, grid computing, pervasive computing, sensor networks, cluster computing, peer to peer computing, wireless sensor networks (Gray, 2008; Afek et al., 2011). These technologies are used for a variety of applications, such as service providing, information processing, resource sharing and data storing and retrieval. In a distributed network, each user tries to utilize or provide the services from/to the other users and the distributed networks are dynamic in nature as well. Moreover, a open distributed network is easy to enter and also susceptible to a variety of malicious attacks (Zahariadis et al., 2010; Sun et al., 2008). Hence, developing a secure protocol to support group communication in a distributed network is a challenging task since there is no concept of a centralized co-ordinator to co-ordinate the activities between different nodes.

In addition to this, each node should also compute and maintain a trust value about other nodes to perform the trust based group communication. Therefore, a new way of trust and secure group key management is needed to detect the existing malicious users in the distributed network. Trust management means, the degree of reliability of the neighbour users, who are used to send the information from source to destination securely. Therefore, we introduce an efficient trust management model in this paper to support the dynamic secure group communication in the distributed networks. In order to develop a trusted group communication, researchers have developed various schemes (Yuxing et al., 2008; Xi et al., 2011; Shaik et al., 2014; Libin et al., 2015). However, most of the schemes suffer from high computational cost since each distributed node has to perform two tasks. One is to generate and distribute the group key to the group users who are in the distributed network. The other work is to compute the trust values for all the users based on the past communication history. Moreover, developing an efficient trust model along with higher trust accuracy is a difficult task. Hence, in this paper, we have proposed a new trust model with high trust accuracy to support the trusted secure group communication. To perform secure group communication, we have already developed two protocols (Pandi et al., 2016; Pandi et al., 2016). In this paper, a new trust evaluation model alone is developed with the following objectives:

- To develop an efficient trust model with high trust accuracy;
- To develop a communication efficient trust model;
- To increase the packet delivery ratio;
- To take a minimum memory space for storing the trust values.

The road map of this paper is represented as follows. The existing security and trust management model is discussed in section 2 and the proposed Trust Level Agreement for Distributed Network (TLADN) is presented in section 3. The Trust evaluation of users is mentioned in section 4, performance evaluation and comparative analysis of the proposed trust management methods are presented in section 5. Finally, section 6 provides the concluding remarks.