An Implementation of Secure Group Communication in a Wireless Environment

M. L. Mat Kiaha, B. Daghighi and S. H. Albakri

Faculty of Computer Science & Information Technology
University of Malaya, Kuala Lumpur, MALAYSIA

misslaiha@um.edu.my, daghighi@gmail.com, sameeralbakri@gmail.com

Keywords: Secure group communication, group key management, and mobile environment.

Abstract. In recent years, group based applications and protocols have gradually gained popularity in term of data traffic distribution across a group of members. Since these applications typically involve communication over open networks, security has become an important requirement. An efficient key management is able to provide confidentiality and integrity of data exchange between group members. This paper is focused to deploy a group key management scheme which is appropriate for wireless environment. From our studies on the existing group key management schemes, decentralized approach is chosen as a desired architecture. The components and their roles, as well as protocols involved in this architecture are described in detail. An implementation of the proposed approach is conducted on mobile devices using Java 2 Mobile Edition (J2ME) while Java 2 Standard Edition (J2SE) is used to enable the communication between key management servers and mobile devices. Different aspects of the proposed scheme in particular the join and leave operations including updating of key materials are then tested and discussed.

Introduction

Ensuring the security of group based applications such as Tele/video-conferencing, stock updates as well as social group networks is no trivial matter since most of group based applications take place over insecure network. Depending on the application need, basic security services such as confidentiality, data integrity and entity authentication need to be in place to ensure backward and forward secrecy, as well as the integrity of group members and group operations. These services in particular the backward and forward secrecy can be established by sharing a common key, which then used to encrypt all traffic of a particular group. Only members of the group can decrypt the received message. Managing a group key is one of fundamental challenges in designing secure and reliable group communication system. There are several group key management schemes for disseminating group key to members of a group, which can be classified into three categories: 1) Centralized 2) Distributed 3) Contributory. Centralized group key management involves a single entity as a group controller responsible for the generation, distribution and updating the group key. Logical Key Hierarchy approach is one of the famous schemes in this category that was proposed by several research groups nearly at the same time [1-2]. Other existing approach can be found in [3-8]. Although adopting centralized approach have some advantages such as 1) easy management because the provision of trust is focused on one entity and 2) some transmission overheads are decreased as member of group need to authenticate the main entity only one time, they suffer from some weaknesses as follows: 1) dependencies on a key server leave a single point of failure, 2) also, it must be constantly available during group operations, and 3) for larger group size, the amount of message transmission between the key manager and group members can be dramatically increased at a same time, which could create bottleneck. In distributed or contributory approach, there is no explicit key entity or centre, and all members contribute to managing the key(s). This approach eliminates the need for central entity while providing uniform distribution of the work load for key management. While it alleviates the single