Journal of Network and Computer Applications 50 (2015) 1–14

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

Toward secure group communication in wireless mobile environments: Issues, solutions, and challenges

Babak Daghighi [a,*], Miss Laiha Mat Kiah [a], Shahaboddin Shamshirband [a], Muhammad Habib Ur Rehman [a]

[a] Faculty of Computer Science and Information Technology, University of Malaya, Malaysia

ARTICLE INFO

Article history:
Received 5 February 2014
Received in revised form
6 September 2014
Accepted 21 November 2014
Available online 29 November 2014

Keywords:
Group key management
Key management
Secure group communication
Host mobility
Wireless

ABSTRACT

Group communication has been increasingly used as an efficient communication mechanism for facilitating emerging applications that require packet delivery from one or many sources to multiple recipients. Due to insecure communication channel, group key management which is a fundamental building block for securing group communication, has received special attention recently. Developing group key management in highly dynamic environments particularly in wireless mobile networks due to their inherent characteristics faces additional challenges. On one hand, the constraint of wireless devices in terms of resources scarcity, and on the other hand the mobility of group members increase the complexity of designing a group key management scheme. The article illustrates a survey of existing group key management schemes that specifically consider the host mobility issue in secure group communication in wireless mobile environments. The primary constraints and challenges introduced by wireless mobile environments are identified in order to show their critical influence in designing a secure group communication. The investigated schemes are then compared and analyzed against some pertinent criteria. Finally, the remaining challenges that should be tackled are outlined, and future research directions are also discussed.

Contents

* Corresponding author.
E-mail address: babak@um.edu.my (B. Daghighi).

http://dx.doi.org/10.1016/j.jnca.2014.11.001
1084-8045/

1. Introduction

There has been a rapid proliferation of wireless communication and portable computing devices due to substantial technological improvements in terms of communication infrastructure, performance, and computing power. Additionally, Internet technology has received the phenomenal advances during the last few years (Sathiaseelan and Crowcroft, 2012). According to a recent study (Cisco Visual Networking Index., 2013), global mobile data traffic will reach 1.4 zettabytes per year by 2017, which may provide inspiration and motivation for the development of new group based applications and services such as multimedia conferencing, interactive group games, video on demand, Internet protocol TV (IP-TV), broadcasting stock quotes, and social group networks (Ganjam and Hui, 2005; Chang et al., 2009; Holzer and Ondrus, 2011; Shin et al., 2013). Group based applications provide an efficient communication by delivering a single copy of data to the network elements such as routers and switches, making copy as necessary for the receivers, which result in a better use of network resources such as bandwidth and buffer space (Hosseini et al., 2007; Shin et al., 2013).

Members can openly and anonymously join the group due to the characteristic of such communications (Martin and Haberman, 2008). Therefore, ensuring the security of group based applications is no trivial matter since lack of security in such applications, taking place over wide and open networks (i.e. Internet) make them more susceptible to numerous attacks (Judge and Ammar, 2003; Sakarindr and Ansari, 2007; Nguyen and Nguyen, 2008). Depending on application requirements, 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 (Sakarindr and Ansari, 2010). These services in particular backward and forward secrecy can be established by sharing a common key (known as a group or traffic encryption key *TEK*). The *TEK* is then used to encrypt all traffic related to a particular group and only members of the group who own the TEK are able to decrypt the received messages. As a result, managing a group key is one of the fundamental challenges in designing a secure and reliable group communication scheme (Baugher et al., 2005).

The extension of group communication to the wireless mobile environment remains difficult and complex in key management protocols. Wireless devices typically suffer from such primary constraints as bandwidth limitations, low computation power, and low storage capacity (Shin et al., 2013). In addition, such devices are able to move from one area of a network to another one, hence member mobility (Biradar and Manvi, 2012; Romdhani et al., 2004; Schmidt et al., 2010) must be considered as an additional parameter in the design of secure group communication. Indeed, user mobility complicates group key management in mobile environments (Koodli, 2009) since key management must deal with both dynamic group memberships as well as dynamic member locations. In wireless mobile environments, the complexity of key management increases when a member moves from one area to another one as the member is not known in the new area. In other words, the mobile member is treated as a leaving member of the group in the departing area and subsequently, as a new member joining the same group in the new area. In these cases, the keying materials must be updated in both areas. This solution creates a communication and computation burden since the updating process is carried out twice thus reducing the efficiency and scalability of the scheme.

Over the last few years, group key management has received attention as an active research area, and several surveys are available that cover various domains of secure group communication such as Rafaeli and Hutchison (2003), Challal and Seba (2005), Sakarindr and Ansari (2007), Zhu and Jajodia (2010) and Sakarindr and Ansari (2010). The surveys in Rafaeli and Hutchison (2003) and Challal and Seba (2005) investigated the solutions available for group key management in wired networks, which were organized into centralized, decentralized and distributed categories. These categories were deduced from the mechanism used for generating the traffic encryption key. The TEK can be generated using either a single or multiple entities or the collaboration of the group members.