Computer Communications 72 (2015) 1–16

Contents lists available at ScienceDirect

Computer Communications

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

Key management paradigm for mobile secure group communications: Issues, solutions, and challenges

Babak Daghighi [a,b,*], Miss Laiha Mat Kiah [a], Shahaboddin Shamshirband [a], Salman Iqbal [a], Parvaneh Asghari [b]

[a] Department of Computer System & Technology, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, KL, Malaysia
[b] Department of Computer Science, Tehran Central Branch, Islamic Azad University, Tehran, Iran

ARTICLE INFO

Article history:
Received 30 June 2014
Revised 17 February 2015
Accepted 7 May 2015
Available online 6 June 2015

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 more sources to multiple recipients. Due to insecure communication channels, group key management which is a fundamental building block for securing group communication, has received increasing attention recently. Developing group key management in highly dynamic environments faces additional challenges particularly in wireless mobile networks due to their inherent complexities. On one hand, the constraints 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. This article illustrates a survey of existing group key management schemes that specifically consider the host mobility issue in secure group communications 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 explored schemes are scrutinized and then compared against some pertinent criteria. Finally, the remaining challenges that should be tackled are outlined, and future research directions are also discussed.

1. Introduction

There has been a rapid proliferation of wireless communication and portable computing devices due to substantial technological improvement in terms of communication infrastructure, performance, and computing power. Besides that Internet technology has received the phenomenal advances during the last few years [1]. According to a recent study, the global mobile data traffic will reach 1.4 ZB per year by 2017 [2], 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 [3–6]. 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 better utilization of network resources such as bandwidth and buffer space [7,4].

Members can openly and anonymously join the group due to the characteristic of such communications [8]. 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 [9–11]. 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 [12]. These services in particular the backward and forward secrecy can be established by sharing a common key (known as group or traffic encryption key *TEK*). The *TEK* is then used to encrypt all traffic of 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 [13].

The extension of group communication to the wireless mobile environment remains more difficult and complex in key management protocols. Wireless devices typically suffer from such primary constraints as bandwidth limitation, low computation power, and low capacity storage [14,4]. In addition, such devices are able to move from one area of a network to another one, hence member mobility [15–17] must be considered as an additional parameter in design of secure group communication. Indeed, user mobility complicates group key management in mobile environments [18] since the key management must deal with both the dynamic group membership as

* Corresponding author. Tel.: +60 172906869.
E-mail address: daghighi@gmail.com, babak@um.edu.my (B. Daghighi).

http://dx.doi.org/10.1016/j.comcom.2015.05.008
0140-3664/

well as dynamic member location. In wireless mobile environment, the complexity of key management would be increased when a member moves from one area to another 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 this case, the keying materials must be updated in both areas. This solution causes the communication and computation burden since the updating process is carried out twice, resultantly reduces the efficiency and scalability of the scheme.

For the last few years, group key management has received attention as an active research area, where several surveys are available in various domains of secure group communication such as [19,20,9,21,12]. Two articles [19,20] have investigated the available solutions of group key management in wired networks, which are organized in three categories, namely centralized, decentralized and distributed. These categories are deduced from the mechanism which is used for generating the traffic encryption key. The TEK can be generated either by a single or multiple entities or the collaboration of the group members.

The study in [12] has listed some secure group communication schemes that offer as many security services (i.e. confidentiality, integrity, non-repudiation and authentication) as feasibly possible. In addition to challenges while establishing secure group communication, there are some known attacks that can severely disrupt group communication over wireless networks which these have all been explored and categorized based on their impacts in terms of data integrity, power consumption, privacy, and service availability in [9]. As such, a number of existing group key management schemes were subsequently presented in three types of wireless environments, namely, infrastructure-based wireless networks, and infrastructureless wireless networks such as ad hoc networks and wireless sensor networks. These efforts are reported to basically reduce communication and computation cost and ward off some particular attacks. In another study, Klaoudatou et al. [22] practically evaluated a number of cluster based group key agreement protocols for wireless sensor network (WSN) applications. The objective of this research was to specify the degree that these protocols impact the performance of the system and energy consumption.

Although the latter efforts explored the secure group communication in wireless networks, the host mobility has not received enough attention. Hence, lack of a survey that investigates the group key managements particularly designed for wireless mobile environments has triggered this research to take off.

This research primarily aims to demonstrate any group key management schemes that offer host mobility protocol for secure group communication in a wireless mobile environment. The respective protocols fall under two categories based on the characteristics of their wireless environment i.e. wireless infrastructure networks (called infrastructure-based) and mobile ad-hoc networks (called infrastructure-less). In addition, this paper identifies the principal constraints and challenges introduced by wireless mobile environment, which have critical influences on designing a secure group communication. By understanding the environment constraints as well as the solution offered for host mobility that exist, it will then be possible to determine what they each have in common and how secure they are and eventually employ this knowledge to build a novel solution. The efficiency and security analysis shows that a number of claims about the security and efficiency of the explored schemes in this research require more clarification.

The organization of the paper is as follows. Section 2 gives an overview of various designing approaches of group key management. The design challenges in mobile wireless environments are investigated in Section 3. The existing group key managements which consider host mobility issues are summarized in Section 4, and subsequently analyzed in Section 5. Section 6 concludes the paper.

2. Taxonomy of group key management approaches

The design of a group key management is a vital component of any security architecture for group communication. The role of entities and processes involved in managing all aspects of cryptography keying materials is specified with a group key management scheme. Depending on who is the designated entity for governing the keying materials, the group key management is distinguished by three approaches as illustrated in Fig. 1: (1) centralized, (2) decentralized and (3) distributed (or known as contributory). In the following subsections, each approach is presented and the underlying common concepts and mechanism are further highlighted in order to identify the advantages and drawbacks of each category.

2.1. Centralized group key management

A single entity referred to as group key manager (GKM) is responsible for generating, distributing and updating the traffic encryption key TEK whenever it is required [13]. This approach is further classified into two categories as illustrated in Fig. 1 depending on the technique used to disseminate the *TEK*. The summary of each category is presented as follows.

2.1.1. Pairwise keys

To manage the keying materials, the GKM shares an individual secret key with each member of the group. This key is used to set up a secure channel between each member and the GKM in order to securely deliver the new *TEK* whenever any changes occur in group membership [23,24]. While maintaining the backward secrecy requires a multicast message, the forward secrecy is assured with $O(n)$ rekeying messages, where n is the number of group members. Thus this solution is not suitable for large and dynamic groups.

2.1.2. Logical Key Hierarchy

Logical Key Hierarchy (*LKH*) approach is one of the famous schemes in this category that was proposed by several research groups nearly at the same time [25,26]. A key server is responsible to maintain a logical key tree. The key tree consists of key nodes and user nodes. The key corresponding to the root of the tree is considered as the traffic encryption key *TEK*. The leaves of the tree are the individual keys which associated with each member of a group. The intermediate keys referred to as key encryption keys (*KEK*) are used by the key server to deliver securely the *TEK* to the group members. Fig. 2 shows a binary hierarchy of keys built for a group with seven members {user1 … user7}. In such schemes, each member must hold the keys on the path from the leaf to the root of the tree, for example member 1 owns {KEK1, KEK12, KEK1234, TEK}.

Using the *KEK*s allow to reduce the required number of update messages specifically when a member leaves the group. As a result, this method can scale to the large group size since the number of messages for updating keying materials is significantly reduced on any changes in group membership. Nevertheless, dependency on a single key server shows a single point of failure and performance bottleneck.

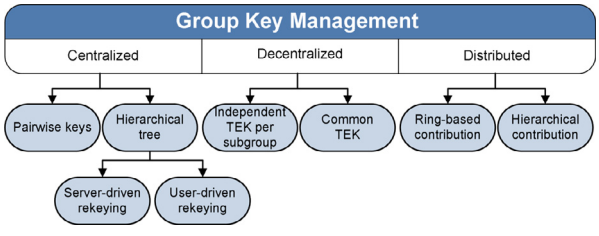

Fig. 1. Taxonomy of group key management protocols.