A novel linear multi-secret sharing scheme for group communication in wireless mesh networks

Ching-Fang Hsu, a,*, Guo-Hua Cui a, Qi Cheng b, Jing Chen c

a College of Computer Science & Technology, Huazhong University of Science and Technology, Wuhan 430074, China
b Institute of Wuhan Digital Engineering, Wuhan 430074, China
c Computer School, Wuhan University, Wuhan 430079, China

A R T I C L E   I N F O

Article history:
Received 9 October 2009
Received in revised form
20 January 2010
Accepted 25 March 2010
Available online 31 March 2010

Keywords:
Wireless mesh networks
Group communication
Ideal linear multi-secret sharing schemes
Monotone span programs

A B S T R A C T

Wireless mesh networks (WMNs) have emerged as an increasingly important technology that offers low-cost community wireless services. The community-oriented nature of WMNs facilitates group applications, such as webcast, distance learning, online gaming, video conferencing, and multimedia broadcasting. Security is critical for the deployment of these services. Secure group communication has become an important component in WMNs. In order to provide secure and efficient group communication in WMNs, in this paper we consider an ideal linear multi-secret sharing scheme, in which each authorized subset may have different target secret. In particular, we put forward a general method of construction for such a scheme by using monotone span programs. The correctness and security of proposed scheme are proved.

© 2010 Elsevier Ltd. All rights reserved.

1. Introduction

Wireless mesh networks (WMNs) have emerged as an increasingly important technology that offers low-cost and high-bandwidth community wireless services. A WMN consists of a set of stationary wireless routers that form a multi-hop wireless backbone, and a set of mobile clients that communicate via the backbone routers. The community-oriented nature of WMNs facilitates group applications, such as webcast, distance learning, online gaming, video conferencing, and multimedia broadcasting. Many of these applications follow a communication pattern in which one or more source clients disseminate data to a changing set of receivers. The openness of the wireless environment makes security a critical concern in the deployment of such group applications.

A major security goal for group applications is providing data confidentiality such that only current group members have access to the data sent to the group. Previous communication must remain protected from newly joined members, and future communication must be protected from members who have left the group. Examples of applications that can benefit from these services are applications which disseminate sensitive content, such as multimedia conferencing, and applications which seek to ensure that only clients that have paid or registered for service can receive data, such as online video broadcasting and distance learning.

In WMNs, during a group communication session, the group members can join or leave the group at any time, with potentially high membership dynamics, possibly due to client movement or flash crowd phenomenon. The focus is on providing data confidentiality from outside adversaries (both passive and active), where an outsider is any non-group member client or backbone router. More specifically, the goal is to provide the group secrecy property, such that it is computationally infeasible for a non-member node (mobile client or backbone router) to discover the group data. This also includes the backward and forward secrecy properties which guarantee that it is computationally infeasible for a member client to gain access to the group data sent before the time it joins the group, or after the time it leaves (or is revoked from) the group, respectively.

Secure group communication is a mature research area and has a large body of research literature. The main objective of a secure group communication protocol is to ensure the data confidentiality against outsiders such that only legitimate group members can recover the group data. In this area the existing works are both in traditional wired networks (see Wong et al., 2000; Torres et al., 2007; Kim et al., 2000, 2001; Steiner et al., 1998; Yiu and Chan, 2004; Abad et al., 2005; Zhu et al., 2005) and in wireless networks (see Zhu et al., 2004; Balachandran et al., 2005; Kaya et al., 2003; Sun et al., 2004; Roy et al., 2005; Curtmola and Nita-Rotaru, 2007), respectively. In general, these schemes in wired networks require reliable communication from each group.