A Multi-service Cluster-Based Decentralized Group Key Management Scheme for High Mobility Users

Trust T. Mapoka, Haider M. AlSabbagh, Yousef A.S. Dama, Simon J. Shepherd, Raed Abd-Alhameed(✉), Mohammad Bin-Melha, and Kelvin O. Anoh

Mobile and Satellite Communications Research Center, University of Bradford, Engineering and Informatics, Bradford, UK
{ttmapoka, sjshepherd, raaabd, oanoh}@bradford.ac.uk

Abstract. Previous cluster based group key management schemes for wireless mobile multicast communication lack efficiency in rekeying the group key if high mobility users concurrently subscribe to multiple multicast services that co-exist in the same network. This paper proposes an efficient multi-service group key management scheme suitable for high mobility users which perform frequent handoffs while participating seamlessly in multiple multicast services. The users are expected to drop subscriptions after multiple cluster visits hence inducing huge key management overhead due to rekeying the previously visited cluster keys. However we adopt our already proposed SMGKM system with completely decentralised authentication and key management functions to address demands for high mobility environment with same level of security and less overhead. Through comparisons with existing schemes and simulations, SMGKM shows resource economy in terms of rekeying communication overhead in high mobility environment with multi-leaves.

Keywords: Mobile multicast communication · Group key management · Wireless networks · Security

1 Introduction

Multicast is an efficient communication technology for the provision of group-oriented services over the internet. These include services such as VOD (Video on Demand) and video conferencing. The services could be deployed more comfortably in wireless mobile networks than in wired networks because the entire receiving nodes within the transmission range of the broadcast medium can receive the services in a single transmission. Thus, the multicast services are expected to be dominating services by considering the fact that majority of the recent standards committees of wireless networks such as E-MBMS in LTE 1 have standardized them. However in order to provide access control to the broadcasted multicast services, a symmetric group key, known as the Traffic Encryption Key (TEK), has been widely deployed to guarantee secure group communications among the subscribed group members. Thus the broadcasted services encrypted by the TEK at the Service Provider (SP) end are

© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2015
S. Mumtaz et al. (Eds.): WICON 2014, LNICST 146, pp. 305–312, 2015.
DOI: 10.1007/978-3-319-18802-7_41