Chapter XII

Key Management for Dynamic Peer Groups in Mobile Ad Hoc Networks

Johann van der Merwe
University of KwaZulu-Natal, South Africa

Dawoud Dawoud
University of KwaZulu-Natal, South Africa

ABSTRACT

Group communication in mobile ad hoc networks (MANETs) generally occurs in the form of dynamic peer groups (DPGs). This chapter reviews the existing group key management schemes for DPGs, found in conventional networks, with respect to their suitability for MANETs. The schemes are uniquely categorized based on their underlying key establishment mechanisms and group topologies. Each group is introduced by presenting the most promising scheme belonging to the subset. The discussions reveal the strengths and weaknesses of the existing schemes and identify the challenges in designing group key management schemes compatible with the unique characteristics of generic MANETs.

INTRODUCTION

Mobile ad hoc networks (MANETs) allow users to establish communication without any fixed or pre-existing infrastructure. The network therefore has no base stations, access points or remote servers. Nodes that are within each others transmission range communicate directly, while relaying the messages for those too far apart. The mobility of the nodes can lead to ‘rapidly changing’ (dynamic) network topologies. Nodes do not have any relationships prior to network formation due to the nature of the applications of MANETs (van der Merwe et al., 2007).

Generic MANETs are created solely by the end-users for a common purpose in an unplanned, i.e. ad hoc fashion. In contrast to conventional networks the users therefore cannot bootstrap the
required security associations with the assistance of a priori shared information on their nodes. This unique property demands distributed collaborative protocols that enable nodes to establish security mechanisms without the assistance of a centralized online Trusted Third Party (TTP).

Many researchers have already proposed peer-to-peer key management schemes that are suitable for self-organized and authority-based MANETs (van der Merwe et al., 2007). In contrast, the available literature contains very few group key management schemes that are designed specifically for MANETs. Authors normally adapt group key management schemes for conventional networks to suite the unique characteristics of MANETs.

The military and commercial applications of MANETs incorporate many group-oriented applications (van der Merwe et al., 2007). The primary subdivision of group key management schemes emerges from the variety of different application dependent group settings that exist in practice. In Figure 1, the two main group key management settings are indicated within the dotted lines, namely:

- Group key management for centrally managed, non-collaborative groups
- Group key management for dynamic peer groups (DPGs)

Large groups, found for example in internet multicast applications, are normally non-collaborative and hard to control on a peer basis (Steiner et al., 2000). They therefore have a structured hierarchy and exhibit one-to-many broadcast communication patterns (Steiner et al., 2000; Kim et al., 2004). The control structure is maintained by a centralized TTP, chosen prior to network formation.

DPGs tend to be relatively small collaborative groups (with membership in the order of a hundred) where all group participants have a symmetric relationship and must therefore be treated equally
Related Content

Medical Quality of Service (m-QoS) and Quality of Experience (m-QoE) for 4G-Health Systems
www.irma-international.org/chapter/medical-quality-service-qos-quality/73144/

Improving Cyber Defense Education through National Standard Alignment: Case Studies
www.irma-international.org/article/improving-cyber-defense-education-through-national-standard-alignment/210625/

Throughput Modeling, Analysis, and Optimization in Cognitive Wireless Networks
www.irma-international.org/chapter/throughput-modeling-analysis-optimization-cognitive/69221/

A Survey of IPv6 Addressing Schemes for Internet of Things
www.irma-international.org/article/a-survey-of-ipv6-addressing-schemes-for-internet-of-things/221334/

Channel State Prediction in Cognitive Radio
www.irma-international.org/chapter/channel-state-prediction-cognitive-radio/69232/