Available online at www.sciencedirect.com
ScienceDirect
Computer Networks 51 (2007) 4303–4321
Computer Networks
www.elsevier.com/locate/comnet

Stateless key distribution for secure intra and inter-group multicast in mobile wireless network ☆

Weichao Wang [a,*], Tylor Stransky [b]

[a] Department of Software and Information Systems, University of North Carolina at Charlotte, Charlotte, NC, United States
[b] Department of EECS, University of Kansas, Lawrence, KS, United States

Received 26 November 2006; received in revised form 5 April 2007; accepted 8 June 2007
Available online 16 June 2007

Responsible Editor: J. Misic

Abstract

Group communication has become an important component in wireless networks. In this paper, we focus on the environments in which multiple groups coexist in the system, and both intra and inter-group multicast traffic must be protected by secret keys. We propose a mechanism that integrates polynomials with stateless secret updates to achieve personal key share distribution and efficient key refreshment during group changes. The proposed mechanism distributes keys via true broadcast. Compared to previous approaches, the proposed mechanism has the following advantages: (1) The adoption of symmetric encryption/decryption for multicast traffic matches the limited processing capability of wireless nodes. (2) The stateless feature of key distribution matches the properties of mobile wireless networks including frequent topology changes and temporary connection disruptions. (3) Special mechanisms are designed to reduce the communication overhead during key updates and provide protection against both intra and inter-group impersonation. The storage, computation, and communication overhead of the proposed mechanism is investigated. Analysis and simulation are conducted to demonstrate the improvements over previous approaches.

Keywords: Stateless key distribution; Secure inter-group multicast; Overhead reduction; Impersonation prevention

1. Introduction

Group communication has become an important component of many applications in mobile wireless networks. It takes advantage of the broadcast characteristic of wireless communication to accelerate information propagation and improve energy efficiency at the mobile nodes when they are equipped with omni-directional antenna. For example, traditional multicast, stateless multicast, and overlay multicast protocols have been developed for wireless networks and a good review can be found in [1]. To prevent attackers from paralyzing the network and services by manipulating and abusing multicast communication, secret keys must be distributed

☆ This research is supported in part by NSF DUE Award #0633143, smart work zone deployment initiative (SWZDI), and KUCR NFGRF. A preliminary version of this work appeared in the proceedings of ACM SASN 2005.

* Corresponding author. Tel.: +1 704 724 0238.
E-mail addresses: weichaow@gmail.com (W. Wang), tstransk@ittc.ku.edu (T. Stransky).

1389-1286/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2007.06.001

and properly maintained throughout the lifetime of the network. Therefore, key establishment and refreshment becomes a critical problem for the applications and must be paid special attention.

In this paper, we focus on the problem of key distribution and update for secure inter-group communication. There are various applications in which the mobile nodes are divided into multiple groups and multicast traffic exists both within the same group and among different groups. Below we describe two examples that can adopt secure inter-group multicast to improve the robustness and efficiency of application level services in wireless networks.

In a United Nations Peacekeeping Operation, three groups of soldiers coming from countries A, B, and C respectively work together to secure an area. Soldiers from the same country or different countries can communicate through multihop wireless connections. Driven by the differences in responsibilities and security clearance levels, when an event is observed by a soldier of country A, descriptions with different contents or different levels of details will be provided to different soldier groups. To support such requirements, a wireless node needs to encrypt its messages with different keys. Secure inter-group multicast is expected in the scenario: only members of the target group could recover the information, and all other nodes should not get access.

Inter-group communication can also be used by soldiers from the same country. We may divide the soldiers into different groups based on their ranks. Each group has its own security level and access right to the information. For example, a soldier may report an event that can be read only by the generals, but not the captains. Secret keys must be deployed to restrict the nodes that can recover the information and participate in the operations.

Enforcing security in these environments puts new challenges to researchers. First, it is different from secure multicast because it involves both intra-group and inter-group communication and multiple keys are required. It is also different from the pair-wise key establishment or pre-distribution methods. Second, membership changes among groups will bring new difficulties to key management. For example, a node may join another group temporarily and switch back later. Therefore, the changes are not necessarily monotonic. Finally, some of the mobile nodes may become temporarily disconnected from the rest of the network because of various reasons such as unreliable communication medium, node movements, and device malfunction. When they are connected again, they should be able to recover the latest keys by passively listening to the broadcast key distribution messages. Therefore, a new approach that supports stateless and efficient key distribution is required to protect multicast traffic in these applications.

A straightforward solution is to deploy a public–private key pair for every group. Every node knows all the public keys and only the private key of the group that it belongs to. For example, for the application described above, a soldier will know Pub_{soldier}, Pub_{captain}, Pub_{general}, and Pri_{soldier}. When he wants to send a message that can be read only by the generals, he can use the Pub_{general} to encrypt the information. To support key updates during group changes, existing approaches such as Logical Key Hierarchy (LKH) [2,3] can be adopted.

This approach is simple, yet with three major disadvantages: (1) Asymmetric encryption, which usually involves exponential computation, must be adopted to protect multicast traffic. It is not efficient for a wireless node when its limited energy and computation capability is considered. (2) When the security level of a mobile node changes or a compromised node is detected and expelled from the current group, secret keys must be updated. It will introduce an overwhelming amount of computation overhead for generating secure public–private key pairs when such changes happen frequently [4]. (3) Since the public keys are known to every node, we cannot determine the identity of the sender based on the encrypted message unless additional authentication methods are adopted. An attacker can easily impersonate another node. This threat is especially severe in inter-group communication since the mobile nodes belonging to different groups usually have weaker trust among each other.

In this paper, we propose a new mechanism that integrates polynomial-based personal key determination with stateless secret update to overcome these difficulties. First, symmetric keys are used to protect the multicast traffic in the same group. At the same time, polynomials are adopted to determine the keys to protect inter-group communication. We calculate the personal key share of a node by applying its unique identity *ID* to the polynomial. When a node changes its group, we adopt the stateless key distribution approaches [5–7] to update secrets via true broadcast. To reduce key update overhead, improve the scalability of the