Available online at www.sciencedirect.com
ScienceDirect
Computer Networks 51 (2007) 69–93
Computer Networks
www.elsevier.com/locate/comnet

A communication–computation efficient group key algorithm for large and dynamic groups

Shanyu Zheng, David Manz, Jim Alves-Foss *

Department of Computer Science, Center for Secure and Dependable Systems, University of Idaho, P.O. Box 441010, Moscow, ID 83844-1010, United States

Received 3 June 2005; received in revised form 21 December 2005; accepted 9 March 2006
Available online 22 May 2006

Responsible Editor: G. Schaefer

Abstract

The management of secure communication among groups of participants requires a set of secure and efficient operations. In this paper we extend existing work to present a Communication–Computation Efficient Group Key Algorithm (CCEGK) designed to provide both efficient communication and computation, addressing performance, security and authentication issues of CCEGK. Additionally, we compare CCEGK with three other leading group key algorithms, EGK, TGDH, and STR. An analytical comparison of all algorithms revealed eight similar methods: add, remove, merge, split, mass add, mass remove, initialize, and key refresh. Comparing the cost in terms of communication and computation, we found CCEGK to be more efficient across the board.

Keywords: Security; Group key management; Group communications; Communication complexity; Cryptographic protocols

1. Introduction

With the advent of new arenas such as wireless ad-hoc and low powered distributed computing and communication devices, designers of group key encryption algorithms can no longer ignore communication in favor of computation or vice versa. In some environments the power cost of communication may be sufficiently high to warrant low cost communication protocols, whereas in other environments computation cost may be the dominant feature. Consequently, this paper introduces the Communication–Computation Efficient Group Key protocol (CCEGK), which is a extension of EGK [1] and TGDH [2,3].

The Communication–Computation Efficient Group Key Algorithm (CCEGK) is a group key management algorithm based upon two preceding group key management algorithms, EGK [1] and TGDH [2,3]. By extending this previous work, CCEGK considerably improves both communication and computation costs of their related operations. Furthermore CCEGK fully implements, as detailed in this paper, several methods that are not

* Corresponding author. Tel.: +1 208 885 5196; fax: +1 208 885 6840.
E-mail address: jimaf@csds.uidaho.edu (J. Alves-Foss).

1389-1286/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2006.03.008