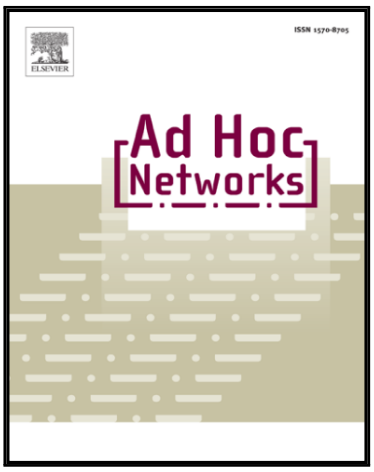

A Secure and Efficient Group Key Agreement Approach for Mobile Ad Hoc Networks

Orhan Ermiş, Şerif Bahtiyar, Emin Anarım, M. Ufuk Çağlayan

PII: S1570-8705(17)30175-0
DOI: 10.1016/j.adhoc.2017.10.003
Reference: ADHOC 1590

To appear in: *Ad Hoc Networks*

Received date: 1 December 2016
Revised date: 3 August 2017
Accepted date: 2 October 2017

Please cite this article as: Orhan Ermiş, Şerif Bahtiyar, Emin Anarım, M. Ufuk Çağlayan, A Secure and Efficient Group Key Agreement Approach for Mobile Ad Hoc Networks, *Ad Hoc Networks* (2017), doi: 10.1016/j.adhoc.2017.10.003

A Secure and Efficient Group Key Agreement Approach for Mobile Ad Hoc Networks

Orhan Ermiş[a], Şerif Bahtiyar[b], Emin Anarım[c], M. Ufuk Çağlayan[a]

[a] *Computer Networks Research Laboratory-NETLAB, Department of Computer Engineering, Bogazici University, 34342, Bebek, Istanbul, Turkey*
[b] *Istanbul Technical University, Faculty of Computer and Informatics, Ayazaga Campus, Maslak, Istanbul, 34469,Turkey*
[c] *Boğaziçi University, Department of Electrical and Electronic Engineering, 80815 Bebek, Istanbul, Turkey*

Abstract

Mobile ad hoc networks have been used in many application areas such as sensors, file sharing and vehicle-to-vehicle communications. Providing secure communications among the users in such networks is a significant issue. Group key agreement protocols are frequently used to provide security in mobile ad hoc networks. There is a number of problems related to the use of group key agreement protocols in mobile ad hoc networks, such as adaptation in cluster-based communications, securely selecting the cluster head for inter-cluster communications, providing secure group key update mechanism for dynamic groups and reducing costs of communications and computations. In this study, we propose a secure and efficient group key agreement protocol that is adaptive for cluster-based communications in mobile ad hoc networks. We describe a novel secure cluster-head selection mechanism in the proposed protocol. The protocol provides security for dynamic group operations in addition to the basic security properties. The proposed protocol also provides better performance in terms of reducing the communications and computational costs. Finally, we present a set of simulations for the proposed protocol in mobile ad hoc networks scenario.

Keywords: Mobile Ad Hoc Networks, Group Key Agreement Protocols, Dynamic Group Operations, Public-Key Cryptography.

1. Introduction

Mobile ad hoc networks (MANETs) have been used in many application areas such as sensors, file sharing and vehicle-to-vehicle communications. Since entities in MANETs are mobile, providing secure communications among participants are significant issue. To overcome this issue, group key exchange protocols are used. Such protocols are categorized as key distribution and key agreement protocols. In key distribution protocols, there exists a centralized authority, such as an entity in the network or a trusted third party, to distribute group keys to participants. In key agreement protocols, all participants in the group compute a shared key by using some public parameters and functions. Since MANETs are decentralized and mobile networks, group key agreement protocols are better candidates than key distribution protocols for providing secure communications.

First, the key exchange protocol has been proposed by Diffie and Hellman, enabling only two participants to agree on a common key in [1]. In [2], two-party secure key exchange is extended to multi-party secure key exchange. After the protocol in [2], various protocols have been published on multi-party setup [3, 4, 5]. Although Burmester and Desmedt in [6] is the most performance-efficient group key agreement protocol in literature, the protocol does not provide authentication property. Authentication is used for confirming the identities of participants in the group communication [7]. In [8], an improved version of Burmester-Desmedt protocol was proposed with authentication and other important security properties such as fault-tolerance and forward secrecy. The fault-tolerance property, which is introduced by Tzeng in [9, 5], is necessary for detecting and correcting the malicious behaviour of participants during key computations. The forward secrecy property is also crucial for providing security against compromising group keys if the long-term private key of any participant is compromised [10, 11]. Tseng's protocol also provides dynamic group operations which are sometimes called as auxiliary group key agreement operations. Such operations are used for efficiently updating the group key without re-executing the protocol for all of the participants in the group [9, 12, 13, 14]. Tseng's protocol is one of the efficient group key agreement protocols since Burmester-Desmedt protocol. However, the protocol has security vulnerabilities against known-key attacks as shown in [15]. In this study, one of our motivation is to improve the security of the protocol against known-key attacks.

MANETs are formed by a combination of clusters. Communications of participants in MANET are categorized as in-cluster and inter-cluster communications. The first one is the communications of participants that are the member of the same cluster. The second one is the communications of participants that are not the member of the same cluster. In order to organize secure communications for such cluster-based network, the most of the existing secure communications protocols use two level security approach [16, 17, 18]. In the two-level security approach, different group key agreement protocols are used for in-cluster communications and inter-cluster communications. Cluster heads become the responsible node for decrypting/encrypting incoming/outgoing messages for inter-cluster com-

*Corresponding author
Email address: orhan.ermis@boun.edu.tr (Orhan Ermiş)