Authenticated and Communication Efficient Group Key Agreement for Clustered Ad Hoc Networks*

Hongsong Shi[1,2], Mingxing He[1], and Zhiguang Qin[2]

[1] School of Mathematics & Computer Engineering,
Xihua University, ChengDu, China
[2] School of Computer Science & Engineering,
University of Electronic Science and Technology of China, ChengDu, China
hongsongshi@gmail.com, he_mingxing64@yahoo.com.cn, qinzg@uestc.edu.cn

Abstract. Common group key agreement protocols are not applicable in ad hoc networks because the dynamic and multi-hop nature. Clustering is a method by which nodes are hierarchically organized based on their relative proximity to one another. Driven by this insight, a hierarchical key agreement protocol is proposed to weaken the 1-hop assumption in common group key agreement protocols. We employ Joux's tripartite protocol and a generalized Diffie-Hellman protocol as the basic building block for group key agreement. The protocol can handle efficiently the dynamic events in ad hoc networks. Moreover, in order to authenticate the messages, a provable ID-based signature scheme is presented. The analysis results indicate that the proposed protocol is secure in withstanding many common attacks and is extremely efficient and feasible to ad hoc networks with large size.

Keywords: Ad hoc networks, Group key agreement, Clustering, Hierarchical routing, Bilinear pairings.

1 Introduction

Recently, mobile ad hoc networks have attracted significant attentions for its wide applications in many different fields. An mobile ad hoc network can be seen as a special dynamic and distributed group, so the secure communication is essential in it. Surely, the most common method is to encrypt messages with a group key only shared by the included nodes, so that those outside the group cannot decode the encrypted messages. Thus, the protocol to achieve the group shared key is crucial, which we often name the *key agreement protocol*.

* This work is supported by the National Natural Science Foundation of China under Grant No.60473030, No.60473090, No.60573129, the Key Projects Foundation of Ministry of Education of China and the Foundation of Science & Technology Agency of Sichuan Province under Grant No.05JY029-131.

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 73–89, 2006.

Over the years, numerous excellent key agreement protocols for dynamic peer group have been proposed [3], such as the GDH suite [18], TGDH [10] and extended STR (ESTR) [11] protocols. However, not all of them are communication efficient when applied to ad hoc networks. Because all of those protocols hold a common implicit assumption that every two nodes can reach each other within one hop. It is reasonable for nodes within the communication range, however those that are far apart have to rely on some intermediary nodes (routers) to relay messages [13]. Ad hoc network with large size is a kind of random networks to which some researches have indicated that the average path length is approximate to $O(\log n)$ (where n is the node count) [1], so communications with multi-hop are inevitable. If the key agreement model is separated from the actual topology of network, a widening gap about the communication complexity between the result of theoretic analysis and the actual application would occur. We call this issue *the neighbors communication problem*.

Recently, Li, Wang and Frieder [13] firstly proposed a hybrid key agreement protocol to solve this problem. In their protocol, the network is divided into some different subgroups based on locations. Each subgroup selects a leader named dominator. Thereafter, the protocol applies the GDH protocol [18] or some other existed group key agreement protocols (e.g. TGDH, Hypercube protocol [13]) in the set of dominators. As a result, the shared key is generated among the dominators. Once it successes, all the dominators distribute the shared key to their relative group members to ensure all nodes share the same key. This protocol provides an efficient method to reduce the neighbors communication problem, however the protocol is inefficient in handling dynamic events and also not suitable for ad hoc networks where the shared key should be the contributions of all the nodes rather than the dominator set. Yao *et al.* [20] proposed a hierarchical key agreement protocol which is similar to [13], i.e., the protocol also divides the network into different clusters and applies some existed group key agreement protocols to construct the group key. The protocol is communication efficient in handling dynamic events, but it is unauthenticated and lack of security analysis. Apparently, this is insufficient when applying to practical situations. However, to some extent, these protocols have casted a new light in finding approaches to weaken the neighbors communication problem.

In this paper, we also present a key agreement protocol for ad hoc networks based on the hierarchical routing protocol. The protocol can handle some dynamic events as node's movements. In order to reduce further the communication complexity, we employ the generalized Diffie-Hellman protocol [7] for two parties and the Joux's protocol [9] for three parties as the fundamental key agreement protocols and extend them for group key agreement. Moreover, we present an provable ID based signature scheme using bilinear pairings to authenticate communication messages. The security and efficiency of the overall protocol are analyzed, it is enough to show that our protocol is secure in withstanding most common attacks and is also efficient in ad hoc networks with large size.

The rest of the paper is organized as follows. Section 2 gives some preliminaries needed to describe our new protocol. Section 3 describes the new key agreement