Accepted Manuscript

An authenticated asymmetric group key agreement based on attribute encryption

Qikun Zhang, Yong Gan, Lu Liu, Xianmin Wang, Xiangyang Luo, Yuanzhang Li

PII: S1084-8045(18)30270-4

DOI: 10.1016/j.jnca.2018.08.013

Reference: YJNCA 2197

To appear in: *Journal of Network and Computer Applications*

Received Date: 6 May 2018

Revised Date: 14 July 2018

Accepted Date: 22 August 2018

Please cite this article as: Zhang, Q., Gan, Y., Liu, L., Wang, X., Luo, X., Li, Y., An authenticated asymmetric group key agreement based on attribute encryption, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2018.08.013.

An authenticated asymmetric group key agreement based on attribute encryption ☆

Qikun Zhang[a], Yong Gan[b], Lu Liu[c], Xianmin Wang[d], Xiangyang Luo[e], Yuanzhang Li[c,*]

[a]School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China.
[b]Zhengzhou Institute of Technology, Zhengzhou 450044, China.
[c]School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China.
[d]School of Computer Science, Guangzhou University, Guangzhou 510006, China.
[e]State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450002, China.

Abstract

Secure communication among terminals in a group is necessary in Internet of Things (IoT). Such as, the Vehicular Ad-hoc Network (VANET) is used to communicate with the vehicles to give alert for weather conditions, road defects, traffic conditions, etc. However, people are also worried about two major security issues: privacy and authentication. Under an open and untrusted network, common secret keys which are negotiated by group terminals through group key agreement are used to realize encryption communication among group members. Personal identity information is exposed and privacy cannot be protected under the traditional identity-based authenticated asymmetric group key agreement protocol. Therefore, an authenticated asymmetric group key agreement based on attribute encryption (ABE-AAGKA) is proposed, which combines the advantages of attribute encryption and identity authentication. Attribute encryption and authentication techniques are adopted to guarantee the secure of group key agreement, and protect the personal privacy. Moreover, calculate and communicate loads are able to be moved to powerful server through the protocol to reduce the workload on intelligent terminal under the imbalanced mobile networks. The proposed protocol is proven to be secure under the inverse computational Diffie-Hellman (ICDH) problem assumption. Performance analysis shows that the proposed scheme is more efficient than existing works.

Keywords: Asymmetric group key agreement; Secure communication; Attribute-based authentication; Personal privacy protection

1. Introduction

Secure group communication is of great importance for many collaborative and distributed Applications in Internet of Things (IoT). such as, the Vehicular Ad-hoc Network (VANET) is used to communicate with the vehicles to give alert for weather conditions, road defects, traffic conditions, etc. However, people are also worried about two major security issues: privacy and authentication [1]. Privacy assures that the communication messages are not intercepted by an eavesdropper, and authentication assures that any unauthorized users cannot fraudulently obtain their required services from home domains.

Group key agreement (GKA) is a secure and robust approach to establish a group key for secure group oriented applications over non-private underlying networks [2]. Group key agreement is one way to ensure the security of group communication for mobile IoT. Asymmetric group key agreement(AGKA) is introduced by [3, 4] to solve the problem. Authenticated key exchange scheme is proposed in [5, 6], which depends on the third party. A new cryptosystem termed as asymmetric group key agreement cryptosystem is proposed by [7, 8]. In this scheme, group members broadcast their contributions to the others by keeping their own information secret. Each group member collects broadcast message from other group participants and derives a common group key.

Dynamic asymmetric group key agreement concerns about the scenarios, such as the terminals in IoT may join or leave at any time. Through designing additional security requirements, the GKA protocol is applicable to dynamic mobile ad-hoc network environ-

*Corresponding author
Email address: popular@bit.edu.cn (Yuanzhang Li)