Cryptology ePrint Archive: Report 2011/216

Secure Group Key Management Approach Based upon N-dimensional Hyper-sphere

Shaohua Tang and Jintai Ding and Zhiming Yang

Abstract: Secure group communication systems become more and more important in many emerging network applications. For a secure group communication system, an efficient and robust group key management approach is essential. In this paper, a new group key management approach with a group controller GC using the theory of hyper-sphere is developed, where a hyper-sphere is constructed for the group and each member in the group corresponds to a point on the hyper-sphere, which can be called the member's private point. The GC computes the central point of the hyper-sphere, whose distance from each member's private point is identical. The central point is published and each member can compute a common group key via the square of the radius. The security relies on the fact that any illegitimate user cannot calculate this value without the legitimate vector, therefore cannot derive the group key. This approach is secure and its backward and forward secrecy can be guaranteed. The performance of our approach is analyzed to demonstrate its advantages in comparison with others, which include: 1) it requires both small memory and little computations for each group member; 2) it can handle massive membership change efficiently with only two re-keying messages, i.e., the central point of the hyper-sphere and a random number; 3) it is very efficient and very scalable for large size groups. Our experiments confirm these advantages and the implementation of our prototype presents very satisfactory performance for large size groups.

Category / Keywords: Group communication, key management, hyper-sphere, security

Date: received 3 May 2011, last revised 8 May 2011

Contact author: shtang at IEEE org

Available formats: PDF | BibTeX Citation

Version: 20110508:093350 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]