Compact and Flexible Resolution of CBT Multicast Key-Distribution

Kanta Matsuura¹, Yuliang Zheng², and Hideki Imai¹

¹ IIS, Univ. of Tokyo, Roppongi 7-22-1, Minato-ku, Tokyo 106, JAPAN
kaata+iis.u-tokyo.ac.jp, imai+iis.u-tokyo.ac.jp

² School of Comp. & Info. Tech., Monash Univ., Melbourne, VIC 3199, AUSTRALIA
yuliang+mars.fcit.monash.edu.au

Abstract. In an open network such as the Internet, multicast security services typically start with group session-key distribution. Considering scalability for group communication among widely-distributed members, we can find a currently-leading approach based on a CBT (Core-Based Tree) routing protocol, where Group Key Distribution Centers (GKDCs) are dynamically constructed during group-member joining process. In search of practical use of it, this paper first analyzes the CBT protocol in terms of its efficiency as well as security management. Then the paper proposes several improvements on the protocol with an aim to solve the problem identified. In particular, (1) an overuse of encryption and signatures is avoided and (2) a hybrid trust model is introduced by a simple mechanism for controlling the GKDC distribution. A comprehensive comparison among the costs of several implementations is also carried out.

1 Introduction

Multicast-oriented applications require a sufficient security infrastructure especially when implemented in an open and global network. A good example is the Internet, where the next-generation protocol IPv6 (Internet Protocol version 6) considers security services for multicast as one of the central issues [1], [2]. The basic starting-point is secure and authenticated distribution or agreement of group session-keys.

A simple strategy is to assign the key-distribution function to a trusted single entity or Key Distribution Center (KDC). This strategy, however, very unlikely scales for multicast communication among widely- or sparsely-distributed members. Scalable approaches would be combined with multicast routing protocols since

– there exist routing protocols which provide dynamic and scalable properties,

– routing mechanisms are typically in close relation to group structures,

and

– combining two pre-processes (routing preparation and key-distribution) potentially saves bandwidth.
Looking at the Internet, we can find IGMP (Internet Group Management Protocol) [3] used in the final delivery of a multicast packet between a local router and a group member on its directly-attached subnetworks. IGMP delivery services can be jointed by a number of different multicast routing and delivery mechanisms among distributed routers.

For groups with dispersed or sparse membership, most scalable are Shared-Tree techniques such as PIM-SM (Protocol-Independent Multicast – Sparse Mode) [4] and CBT (Core-Based Tree) routing protocol [5]–[7]. The main differences between these two techniques are that

- CBT maintains its characteristics as scalable as possible by not offering the option of shifting from a Shared Tree to a Shortest Path Tree

and that

- CBT has fewer entries in the routing tables [8].

Thus, although not devoted to any specific implementation, a dynamic key-distribution protocol in conjunction with CBT [9] is currently considered as a strong candidate for a scalable multicast key-distribution scheme. This protocol uses Group Key Distribution Centers (GKDCs) which are dynamically constructed during group-member joining process.

This paper first overviews the CBT mechanism in Sect. 2, where several problems or questions are subsequently discussed, and finally four implementations are evaluated in terms of their computational costs and communication overhead. A more compact and yet more flexible resolution is then proposed in Sect. 3 with a function of controlling GKDCs, followed by the evaluation of four implementations. After discussion in Sect. 4, Sect. 5 gives conclusions.

2 Core-Based Tree

2.1 Routing Protocol

In the CBT routing protocol [5]–[7], a single shared delivery tree is built around several core routers. When a host wishes to join the multicast group, it casts an IGMP group membership report across its attached link. On receiving this report, a local CBT-aware router explicitly joins the delivery tree by generating a JOIN_REQUEST message, which is sent to the next hop on the path towards one of the group's core routers. In reply to this JOIN_REQUEST message, a JOIN_ACK message is generated by the core or another router which has already joined the tree on the path between the core and the host. This JOIN_ACK message traverses the reverse path of the join and thus a new branch is created. Routers along the new branch are called non-core routers, and there exists a parent-child relationship between adjacent routers along the branch. The resulting tree is a bidirectional and acyclic graph that reaches every member host. Once the tree is established, packets are forwarded in a simple way: when a node receives a