Wireless Pers Commun (2010) 55:35–49
DOI 10.1007/s11277-009-9784-2

PIMac: Multicast Access Control Implementation in PIM-SM

Xin Li · Hongke Zhang · Jian-Ming Chang · Jiann-Liang Chen · Han-Chieh Chao

Published online: 4 August 2009

Abstract In this paper, we present an access control scheme for PIM-SM multicast domain. In order to avoid the overhead of digital signature algorithm, the proposed solution makes use of the Rendezvous Point to collect keys and implement a distributed shared-key based multicast access control system. As it supplies efficient host access control in PIM-SM domain, we name this scheme PIMac. Compared with the existing multicast admission control solutions, PIMac has following advantages: (1) support both receiver and sender access control; (2) realize host exclusion based on expire time; (3) compatibility with current PIM-SM protocol; (4) lower join latency; (5) anti-replay and DoS robustness; last but not least, (6) PIMac architecture is divided into two separated domains: AAA domain and multicast routing domain, entities in each domain do not rely on PKI interoperability or common secret to authenticate

X. Li · H. Zhang
National Engineering Laboratory for Next Generation Internet Interconnection Devices,
Beijing Jiaotong University, Beijing, People's Republic of China

J.-M. Chang · J.-L. Chen
Department of Computer Science & Information Engineering, National Dong Hwa University, Hualien, Taiwan

J.-L. Chen
Department of Electrical Engineering, National Taiwan University of Science & Technology, Taipei, Taiwan

H.-C. Chao
Department of Electronic Engineering, Institute of Computer Science & Information Engineering, National Ilan University, I-Lan, Taiwan

H.-C. Chao
Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan

X. Li (✉)
School of Electronics and Information Engineering, Beijing Jiaotong University, 602 Room,
South of No. 9 Teach Building, 100044 Beijing, People's Republic of China
e-mail: lixin.biz@gmail.com

each other. The experimental results show that PIMac achieves flexible manageability and improves the performance of multicast access control systems effectively.

Keywords IP multicast · Rendezvous point (RP) · Routing security · Access control · PIM-SM

1 Introduction

The routing security issue is still largely open while multicast routing protocols, such as PIM-SM [6], have been widely deployed. Though Internet Service Providers (ISP) and Content Providers (CP) are very interested in multicast applications, the difficulty of multicast authentication, authorization and accounting (AAA) has become one of the main reasons which prevent IP multicast from being widely accepted and commercially applied. Unlike unicast, the data packet delivery path in multicast routing is not only determined by routing infrastructure but any terminal host can change the shape of multicast delivery tree by sending normal IGMP/MLD group membership request to multicast Designated Routers (DRs). The open join/leave service model of IP multicast makes routing security issues totally different from traditional unicast routing security: In the case of unicast routing, routers notify each other with the attached network prefixes. Based on this network address information, path computing algorithms are used to compute the route to a given destination network. Protecting the unicast routing protocol messages from being altered or forged is enough for unicast routing security. In the case of open multicast routing model, though the similar mechanism [20] as the above unicast (all the multicast routers (MRs) are required to share a secret and apply symmetrical signature algorithm to authenticate the routing control packages to and from each other) has been proposed to protect multicast routing protocol messages and effectively avoid router spoofing attack, the multicast delivery path can still be maliciously changed in spite of all packets between MRs are secured. MRs at the edge of IP multicast network allow any host join and leave groups at any time without performing admission/access control or keeping the host's identification information. Typically, current multicast routing infrastructure is fragile when suffering following attacks:

(1) Malicious hosts can send forged or meaningless multicast datagram.
Risk: The illegal multicast packets will be delivered to multiple receivers, wasting network resource all along the delivery path in wide area and disturbing legal multicast session. DoS attack may be caused against routers or receivers.

(2) Malicious hosts can send forged or normal IGMP/MLD Report to join a multicast group in the subnet where no valid receiver is present.
Risk: The multicast delivery tree is forced to extend new branches to unintended subnets where multicast datagram will also be forwarded to. Network bandwidth is wasted and the packets of multicast session are received by unauthenticated hosts, content will be revealed if no encryption technique is applied.

(3) Flooding MRs in the edge with IGMP/MLD Join/Report message of large number of different multicast groups.
Risk: Dynamic multicast routing protocols like PIM require MRs to maintain the state for every joined group. Holding these routing states for a large number of unauthenticated groups wastes the resource in MRs and DoS attack can be easily achieved when fringe MR suffers from IGMP flooding.

(4) Sending forged IGMP/MLD leave message to MR.

Risk: Valid user in the same subnet where attacker exists can be forced to leave multicast group. The continuity of multicast session is affected.

In recent years, many end-to-end security mechanisms [12] and group key management (e.g., [14]) have been proposed to secure group communication. They achieve encryption and authentication of multicast packets to ensure data confidentiality, integrity and origin authentication with non-repudiation proof. The information security of group communication is achieved by these means, however, the security hole in IP multicast routing infrastructure still exists. The basic solution to this problem is providing access control service for IP multicast.

The rest of the paper is organized as follows. In Sect. 2, we outline the existing multicast access control solutions, classify them and summarize limitations and advantages of each approach. In Sect. 3 an innovative multicast access control system named PIMac is presented; we describe the motivation, design requirements and architecture; PIMac implementation and the extension to PIM-SM are also given. In Sect. 4 we compare PIMac with existing solutions, give performance analysis and numerical results. Finally in Sect. 5 we conclude our research with summary.

2 Overview of Multicast Access Control

We classify the existing multicast access control approaches into two classes (Fig. 1): asymmetric signature based and symmetric signature (shared key) based solutions. In the asymmetric signature-based schemes, such as Basic RAC [4], Gothic [11], and G-CBA [5], a central group management server (GM) performs user authentication and authorization and then grants valid user with an access control certification which is signed with GM's private key. When host wants to join a controlled multicast session, it has to send IGMP/MLD Join request together with the received certification [9]. When receiving the request, multicast Designated Router (DR) verifies the signature of certification with GM's public key and then performs access control according to the information contained in the certification. The form of certification may vary, for example, G-CBA uses Cryptographically Based Address (CBA) [1] as certification which can be authenticated by the public key of issuer (GM).

In the symmetric signature based solution, host and router authenticate each other based on shared secret information which is typically known by those entities exclusively. In literature [10], authors propose a symmetric key based scheme. This scheme denoted here as IGMP-auth extends IGMP protocol and DR's function to perform user access control. Endpoint Hosts submit multicast send or receive request along with its own authentication information

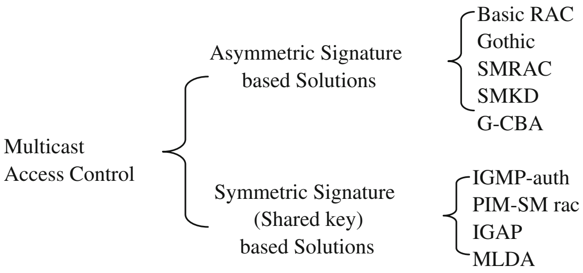

Fig. 1 Multicast access control schemes