TELKOMNIKA, Vol.11, No.3, March 2013, pp. 1298 ~ 1304
ISSN: 2302-4046

Service-oriented Controllable Multicast Model for Next Generation Internet

Ye Zhao[1], Hu Jinlong[*2], Zhang Ling[3]
[1, 2]Network Engineering and Research Center,
South china University of Technology,Guangzhou, China
[3]Communication and Computer Network Laboratory of Guangdong Province,
South China University of Technology
Corresponding author, e-mail: zhye@scut.edu.cn[1], jlhu@scut.edu.cn[2], ling@scut.edu.cn[3]

Abstract

With the development of the IPv6 networks, more and more applications put forward to use multicast. Multicast security and management is one of the key issues for IP multicast services deployment in IPv6 network as in IPv4 network. We introduce the idea of Service-Oriented Architecture (SOA) in software scope to multicast service, and design a Service-oriented Controllable Multicast Model (SOCMM) for IPv6 multicast services. And the reference implementation of this model is proposed in this pape.

Keywords*: Controllable Multicast, Service-oriented Architecture, IPv6, Next Generation Internet*

1. Introduction

Multicast is an effective way for one-to-many or many-to-many communication. S. Deering defined the IP multicast model in 1989 [1]. There are two kinds of IP multicast, including Any-Source Multicast (ASM) Model [1] and Source-Specific Multicast (SSM) Model [2]. Although IP multicast has many advantages such as high efficient forwarding, low load for the servers and network [3], there exists scalability, security and management problems, which highly limit the large scale development of IPv4 multicast.

There are some new features in IPv6 multicast compared with IPv4 multicast. In IPv6 network, IPv6 routers are required to support multicast, while multicast is optional in IPv4 routers. In addition, IPv6 multicast has huge address space, and it has a 4-bit field called scope to support multicast service more flexible. And IPv6 multicast supports Embedded RP, which inserts RP address into IPv6 multicast address, so that routers can extract RP address directly and using shared tree immediately.

However, multicast service has many security and management challenges, espe-cially in IPv6 multicast environment. Since IPv6 multicast has no restrict on group member as same as IPv4 multicast, attackers could fake to be legal members, and there is no mechanism in multicast to prevent members or non-members to send packets to one multicast group, which easily leads to DoS attacks. Even more, comparing with unicast communication, multicast packets are transferred in a more network, which gives attackers more opportunities to intercept and eavesdrop packets.

With the development of the next generation Internet, new applications put for-ward higher requirements for multicast security and management mechanism. Al-though people study source authentication, sender access control, receiver access control, group key management, multicast secure routing and other aspects [4-5, 7], there is few effective and unified large-scale multicast service solutions for multicast group management, multicast address allocation, multicast admission control and multicast transmission control in open multicast model.

The rest of the paper is organized as follows. Section II describes the related work. The model design and the reference implementation of this model is describes in section III. Section IV concludes the paper

Received October 13, 2012; Revised January 10, 2013; Accepted January 21, 2013

2. Related Work

Securing IP multicast group communication is a complex task that involves many aspects. Internet Engineering Task Force (IETF) has set up Multicast Security (MSEC) Working Group, and Multicast Backbone Deployment (MBONED) Working Group to address different aspects of the multicast security solution, such as multicast security architecture and multicast key management.

Hardjono and Weis proposed a Multicast Group Security Architecture (MGSA) for large-scale multicast environment, which includes a centralized multicast secu-rity reference framework and a distributed security reference framework. Baugher introduced a general structure about multicast security group key, Group Security Association (GSA) and a protocol to build GSA key management. In order to describe the application requirements of multi-entity Content Delivery System (CDS), Hayashi divide CDS multicast commercial model into three parts, and lists the requirements of the three mode [6]. Satou proposed a multicast au-thentication, authorization and accouting framework (MultiAAA), which includes basic model and full function model [7].

Although MGSA architecture and MultiAAA framework clearly describe each functional element in multicast security services, there are still many challenges to effectively manage and control large-scale IP multicast and to provide efficient multicast service in the open Internet environment.

On the other side, in order to adapt to new business, new application and devel-opment of information technology, people research new network architecture from the aspects of service-oriented and application-oriented rather than transmission-oriented, such as service-oriented network architecture [8], serve as the center of the network [9], Service Oriented Network Architecture (SONA) [10].

There are some works about service-oriented network protocols combination and network service abstraction, such as Baldine et al. proposed SLIO structure [11-12], Wolf et al. proposed a method like pipeline to define network service [13]. There also some work about Distributed Monitoring and Controlling method in internet or Multi Service Networks [14] [15]. But there is few of work focused on the service-oriented multicast for Next Generation Internet.

3. Service-Oriented Controllable Multicast Model

3.1. Model Design

There are more and more requirements about security and quality for multicast applications, such as IPTV, HD video meeting. Traditional multicast applications based on the “Best-Effort” network. Network was considered as a simple connec-tor among terminals, which makes network difficult to provide multicast service security and quality.

In order to improve multicast service security and quality, there are various func-tional modules have been patch to the network, which make the network more complex and difficult to control, and blocks multicast applications to be widely deployed. Multicast service needs a more flexible and controllable network which could ensure security and quality.

In the scope of software, Service-Oriented Architecture (SOA) is a set of principles and methods to design and develop inter-operable service software [13]. The key technical concept of SOA includes service, interoperability and loose coupling. These services clearly define business functionality and implemented by reusable software components. The goal of SOA is to build a large-scale distributed system based on the abstraction of business rules and functions. In practice, the description of the services generally starts from interface definition. The service interface definition could be made from different perspectives. SOA tends to busi-ness-driven interface rather than technology-driven interface, which means more focused on demand-based design rather than implement-based design.

In this paper, we bring service-oriented concept of software into the multicast ser-vice. As shown in Figure 1, video conferencing, IPTV, multi-games and other high-level multicast service users could use controllable multicast network service through the interface provided by the underlying multicast network.

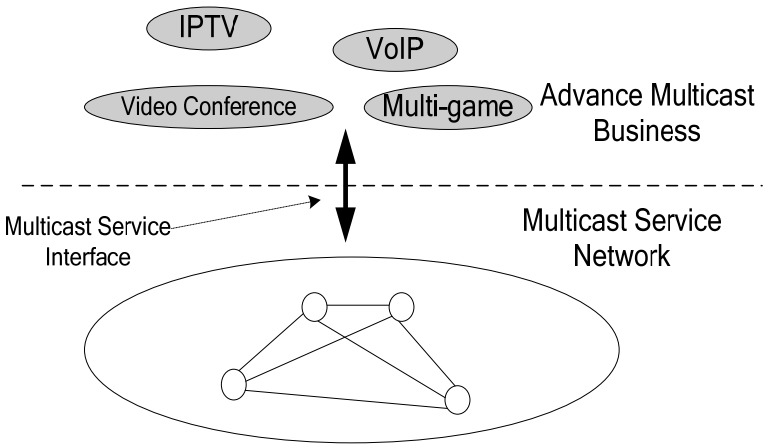

Figure 1. Business-driven Multicast Service

Overall, business-driven multicast service provides multicast service users an abstract mechanism, which reliefs the multicast service users from the heavy mul-ticast service security and management job.

In order to do a rational and simple description, we propose a Service-oriented Controllable Multicast Model (SOCMM) in this paper. SOCMM defines the archi-tecture of multicast service system, relationship between each layer, and the ser-vices in each layer. Multicast service provider could offer more controllable mul-ticast service through SOCMM.

As shown in Figure 2, SOCMM divides multicast service into three layers logi-cally, including Multicast Infrastructure Layer (MIL), Multicast Service Layer (MSL) and Multicast Business Layer(MBL).

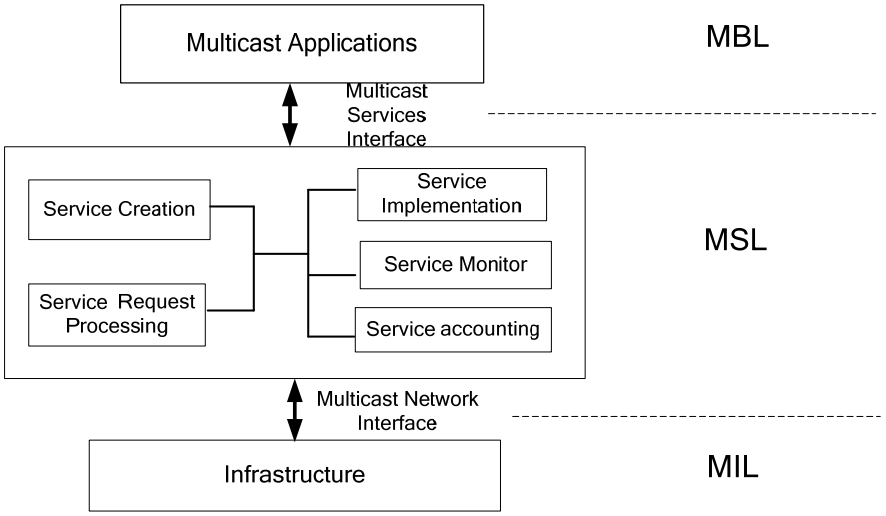

Figure 2. Service-oriented Controllable Multicast Model

MIL mainly includes network infrastructures such as multicast network switch, multicast router. It provides basic multicast network functions.

MSL is the middle layer of SOCMM. It is supported by MIL and provides multi-cast service functions, such as the creation of multicast service, handle of multi-cast service request, implementation of multicast service, multicast service moni-tor and accounting and et al.

MBL is the top layer of SCOMM, which is also called multicast application layer. It implements multicast business through interfaces provided by MSL to meet the demand of HD video conference, IPTV and so on.

In SCOMM model, service is as an implement of self-sufficient multicast busi-ness, and hides technical details to make multicast applications easier to use the multicast service. And the users could pay more attention to business.

Each layer in SOCMM uses services provided by lower layer, and provides ser-vices to upper layer. In SOCMM, there are two interface including Multicast Net-work Infrastructure Interface (MNI) and Multicast Service Interface (MSL). MNI is located between MIL and MSL, which is used for MSL to control and manage multicast router and switch in MIL. MSI is located between MSL and MBL, which is the interface for MSL to provide multicast service to MBL.

3.2. Reference Implementation

In the backbone and campus network environment, we propose an implementation program of SOCMM model using open network protocols, as shown in Figure 3.

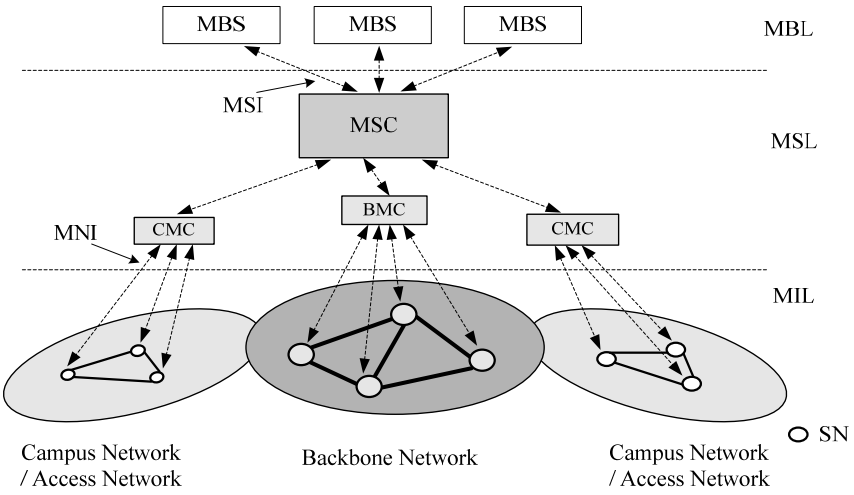

Figure 3. SOCMM Reference Scheme

In MIL layer, the multicast network consists of multicast backbone network and some connected campus network/access network. In multicast network, multicast service element is called Service Node (SN), which includes controllable network equipments such as multicast router and multicast switch.

In MSL layer, a set of multicast service controllers manage multicast network service node through MMI interfaces, and provide multicast service to various multicast business through MSI interfaces. Service controller mainly consists of Multicast Service Controller (MSC), Backbone Multicast Controller (BMC) and Campus Multicast Controller (CMC).

In MBL layer, MBS uses all multicast services provided by lower layer through MSI interfaces in MBL; In MSL layer, CMC and BMC can control and manage controllable multicast network equipments through MNI interfaces.

3.2.1. Service Controller

Multicast Service Controller(MSC)

MSC is the master controller of SOCMM, and provides multicast service interfac-es for multicast service users. As shown in Figure 4, Multicast Management Mod-ule (MMM) is in charge of multicast address distribution; Multicast Security Module (MSM) is in charge of key

management, such as key creation, key update, key destroy and key distribution, and coordinates CMC to manage multicast group access; Multicast Resource Module (MRM) is mainly used to coordinates BMC and CMC to distribute and guarantee band resource.

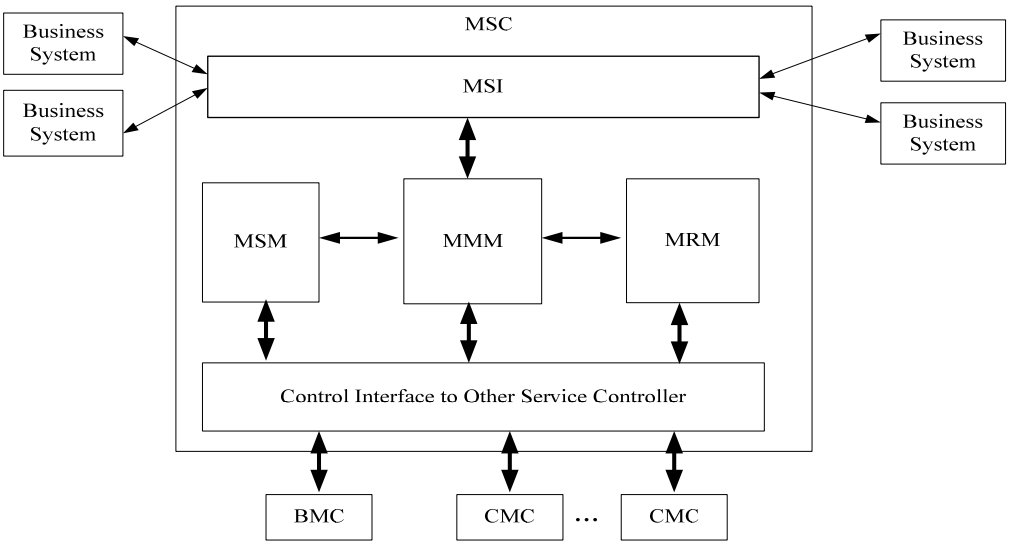

Figure 4. Multicast Service Controller

Backbone Multicast Controller（BMC）

BMC is the controller of multicast backbone network. It is mainly used to coordinate with multicast resource module of MSC and to coordinate multicast network resources such as multicast forwarding, bandwidth allocation and guarantee in backbone network by controlling the multicast router.

Campus Multicast Controller（CMC）

CMC is the controller of campus network or access network, mainly used to coordinate with multicast security module of MSC, to control multicast sources in campus network or access network and multicast members joining and leaving.

CMC could stop unauthorized multicast stream sending by taking strict control over multicast sources, and stop specified uses to fetch unauthorized multicast stream by taking strict control over multicast receivers.

3.2.2. Service Node (SN)

SN is network equipment used to multicast forwarding, mainly including mul-ticast routers and multicast switches.

In order to realize remote control on multicast equipments, the new multicast network equipments architecture is as shown in Figure 5. Multicast Control Agent (MCA) could interact with other multicast modules in multicast equipments to realize controlling over each multicast function in equipments; Multicast Control Interface (MCI) is an interface between MCA and network controller, which rea-lizes remote control over each multicast functions in equipments.

3.2.3. Workflow

As shown in Figure 6, before running a multicast business, MBS should send requests, such as security demand, multicast source address, bandwidth demand, multicast member node, service time and so on, to MCS through MSI. MCS as-sess the multicast business to determine whether the current resources can meet the requirements, and provide relative information to the multicast source.

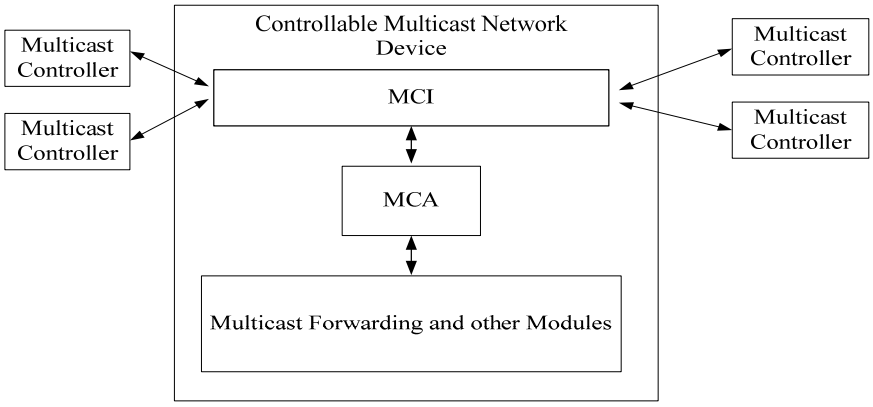

Figure 5. Architecture of Multicast Service Node

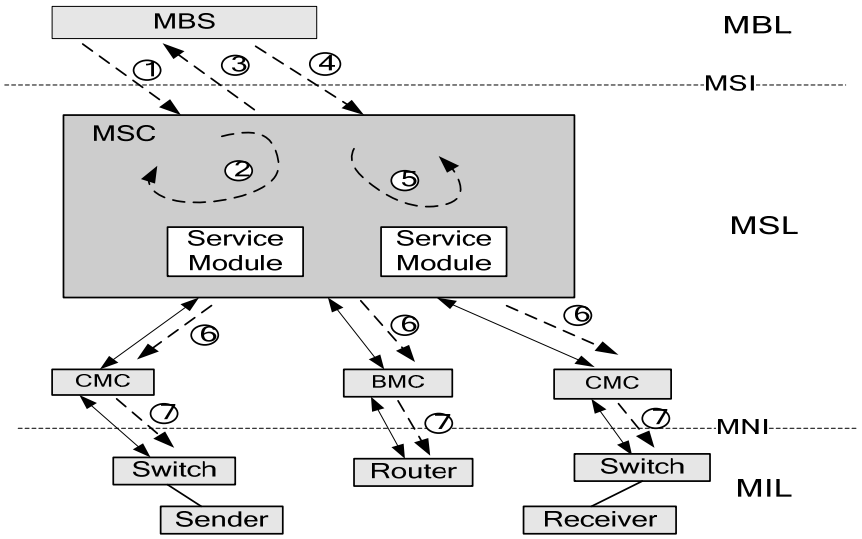

Figure 6. Workflow of SOCMM

MCS configures multicast control rules on the edge switch directly connected with the multicast source and multicast receivers via CMC to achieve controlling over multicast members. Multicast access control switch needs to realize flexible con-trol over multicast sources sending data and multicast receivers receiving data, as well as control agent to interact with CMC.

4. Discussions

Comparing with service-oriented network architectures such as SONA, SOCMM is designed for multicast service model, and describes three logic layers in multicast service. It explicitly introduces the concept of software-oriented ser-vices into controllable multicast model design. Business of application layer mul-ticast service interface MSI uses multicast service.

Compared with traditional multicast security solutions such as MSGA, SOCMM program considers the multicast service security and management prob-lems of the next generation large-scale Internet from the service-oriented view, but not limit to the security of multicast key management architecture.

In secure multicast communication environment, SOCMM program protects the security of multicast from the process of multicast data stream transmission, such as multicast

admission control and multicast transmission security. In multi-cast business developing, SOCMM uses service-oriented structure, hides technol-ogy details, and it is also easily developed and integrated with other systems.

5. Conclusion

Enhancing controllable is helpful to build a more security and more trust IPv6 multicast network. Although there are many security multicast schemes have been proposed, there are few of papers discuss how to build a controllable multicast. Combine with SOA in the scope of software, we designed a novel controllable multicast model—SOCMM, and a reference implementation of SOCMM. With the more widespread deployment of IPv6 networks, controllable multicast would be an important feature for Next Generation Internet in the future. Using the Service-Oriented Architecture to improve the security and controllability of multicast has produced many opportunities and challenges to further study, such as the multicast service assurance and service composition.

Acknowledgment

This work was supported by the State Key Development Program for Basic Research of China (NO.2009CB320505) and the Fundamental Research Funds for the Central Universities (NO.2012ZM0094).

References

[1] S Deering. IETF RFC 1112. *Host Extensions for IP Multicasting*. 1989.
[2] S Bhattacharyya. An Overview of Source-Specific Multicast (SSM). *IETF RFC 3569*. 2003.
[3] C Metz, M Tatipamula. A Look at Native IPv6 Multicast. *IEEE Internet Computing*. 2004; 8: 48-53.
[4] T Hardjono, B Weis. The Multicast Group Security Architecture. *IETF RFC 3740*. 2004.
[5] M Baugher, R Canetti, L Dondeti. Multicast Security (MSEC) Group Key Management Architecture. *IETF RFC 4046*. 2005.
[6] T Hayashi, H Satou, H Ohta, et al. Requirements for Multicast AAA coordinated between Content Provider(s) and Network Service Provider(s). *IETF draft-ietf-mboned-maccnt-req-10*. 2010.
[7] H Satou, H Ohta, T Hayashi, et al. AAA and Admission Control Framework for Multicasting. *IETF draft-ietf-mboned-multiaaa-framework-12*. 2010.
[8] B Reuther, P Müller. Future Internet Architecture–A Service Oriented Approach. *Information Technology*. 2008; 50: 383-389.
[9] T Braun, V Hilt, M Hofmann, et al. Service-Centric Networking. *2011 IEEE International Conference on Communications Workshops (ICC)*, Washington. 2011.
[10] *Cisco System Corporation, Service Oriented Network Architecture (SONA)*, http://www.cisco.com/en/US/netsol/ns629/index.html.
[11] I Baldine, M Vellala, A Wang, et al. *A unified software architecture to enable cross-layer design in the future internet*. In Proceedings of Sixteenth IEEE International Confe-rence on Computer Communications and Networks (ICCCN), Washington. 2007; 26-32.
[12] R Dutta, GN Rouskas, I Baldine, et al. *The SILO architecture for services integration, control, and optimization for the future internet*. In Proceedings of IEEE International Conference on Communications (ICC), Washington. 2007; 1899–1904.
[13] Shanbhag S, Wolf T. Implementation of end-to-end abstractions in a network service architecture. *In Fourth Conference on emerging Networking EXperiments and Technologies (CoNEXT*), ACM. 2008; 1-12.
[14] A Ashar. Distributed Monitoring and Controlling Using Microcontroller and Virtual In-ternet Protocol. TELKOMNIKA. 2010; 8(1).
[15] FM Puspita, KS BM Taib, Z Shafii. An Improved Optimization Model of Internet Charging Scheme in Multi Service Networks. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(3): 592-598.