AoS: A Scalable Architecture for Inter-Domain IP Multicast

Yuncheng Zhu Hongqiang Liu Congxiao Bao Xing Li
Network Research Center, Tsinghua University, Beijing 100084
{zhuyc07,liuhq07}@mails.tsinghua.edu.cn  {congxiao,xing}@cernet.edu.cn

Abstract—IP multicast originally works in Any Source Multicast (ASM) that comes with great burden and dynamics on the backbone routers and weakness in inter-domain scalability. It also brought serious security and management problems. In contrast, Source-Specific Multicast (SSM) has been recognized as a simple, scalable and secure method, especially in inter-domain multicast. Therefore, MSDP is no longer needed. The major weakness in MSR's addresses [5] are embedded into ASM group addresses, domains, and in IPv6, domain's unicast address prefixes or RP's addresses [5] are embedded into ASM group addresses, therefore MSDP is no longer needed. The major weakness in scalability of ASM comes from MSDP’s flooding mechanism for sender announcement, which cannot handle the great amount of dynamic sources internet-wide. Although MSDP is abolished in IPv6, those mechanisms violate the domain independence, and potentially the interest of an Internet Service Provider (ISP), in that an RP must treat the senders of other domains. Furthermore, ASM has brought serious security and management problems into multicast [6].

In contrast, Source-Specific Multicast (SSM) [7] was proposed to endow the receivers with the ability to specify data sources. With Internet Group Management Protocol version 3 (IGMPv3) [8] in IPv4 and Multicast Listener Discovery version 2 (MLDv2) [9] in IPv6, receivers join channels by specifying both senders S and groups G, and they can block/unblock any source S at any time. SSM has been recognized as a simple, scalable and secure method, especially in inter-domain multicast. However, there are some new problems rising with its benefits. Firstly, SSM routers must keep as many forwarding states as \((S \times G)\), which consumes large amounts of routers’ memory. Secondly, although SSM is suitable for one-to-many applications such as IPTV, but many-to-many applications such as online games and video conferences embody an ASM nature. Therefore, deployment of SSM often stagnates, as a result of inadequate demand from SSM-enabled applications and operating systems.

In this paper, we propose ASM-over-SSM (AoS) architecture as a solution for scalable inter-domain multicast. The basic idea of AoS is building a two-tier hierarchy in a multicast-enabled internet. The tier-1 part is provider networks, which are often transit backbones. They interconnect each other using only SSM. The tier-2 part is customer networks attached to tier-1 through AoS gateway and could support both ASM and SSM applications at the same time. AoS not only combines the advantages of both ASM and SSM, but also achieves:

- Dynamics and complexity of core routers is mitigated.
- Routing states are reduced so that inter-domain multicast scales.
- No modification on current multicast routers is required.
- Current multicast applications are well supported.

In the following parts of the paper, we’ll firstly (in Sect. II) identify the requirements of the new model of inter-domain multicast architecture. In Sect. III, we focus on the design of its architecture and gateway. A comprehensive evaluation is also presented in Sect. IV before the paper is concluded.
II. DESIGN REQUIREMENTS

To tackle the scalability and stability problems current multicast is facing with the support to many-to-many multicast applications, we propose a novel inter-domain multicast architecture where the backbone domain is a SSM only one, and subnets supporting ASM is connected to it with our AoS gateways. Regarding the understanding on the scenario where AoS is required, there are several criteria that the design of a new architecture like AoS should satisfy.

A. Transparency

Any host in any subnet running some multicast application, especially ASM application, should be able to send/receive multicast packets towards/from host in any other subnets. That is to say, the AoS architecture should be transparent to currently widely deployed multicast applications. Otherwise, users would be hesitated to migrate to the new architecture for the concern of losing accessibility, which is similar to current problem with SSM deployment.

B. Compatibility

AoS architecture should be compatible with current IP multicast routing protocols, so that there is no modification required on routers. This could guarantee that the security and management mechanism of current protocols would not be tampered by new architecture. Besides, this avoids ISP from upgrading hardware or software of current routing facilities.

C. Scalability

According to current practice of many-to-many ASM applications, there would be a number of sources in one multicast session, for example, several hundreds. Moreover, the amount of receivers could be very large, and receivers could be scattered in different ASM-supported subnets. Hence, AoS architecture should be scalable to support multiple sources and up to infinite receivers for each multicast session.

D. Management

Any network using AoS architecture should be able to be managed efficiently. For example, traffic control and security authentication should be easily performed to permit the communication of authorized multicast groups only. Besides, the gateway of AoS shouldn’t demolish the authenticity of network addresses, and shouldn’t be vulnerable to malicious attacks.

III. ARCHITECTURE

According to the design requirements, the AoS architecture is built to separate the inter-domain multicast into SSM-only backbone parts and ASM-supported subnet parts. In this section, we present the design and features of AoS and the detailed functionality of its gateway.
Fig. 2. Communication process of a multicast session in AoS

B. Procedure

Before digging into the details of the gateway, we first illustrate how AoS works with a typical example. For simplicity, we assume that two hosts, Amy and Bob, in different subnets would participate in a ASM session, as shown in Fig. 2.

Without the help from AoS gateways, Amy and Bob cannot communicate with each other although they are agree to use the same ASM group \((*, G1)\), because they are located in different ASM “islands”. In order to serve this multicast session, gateway \(S1\) needs to join the ASM group \((*, G1)\) to receive data sent by Amy, and gateway \(S2\) needs to join a SSM group \((S1, G2)\), where \(G2\) is an equivalent group address of \(G1\) in SSM, to relay the data from \(S1\). When those preparations are done, the two hosts could communication through:

1) Amy sends a UDP packet towards \(G1\).
2) Gateway \(S1\) receives this packet.
3) \(S1\) forwards the packet to backbone with small modifications: source address changed into the address of \(S1\) and group address changed into \(G2\).
4) Gateway \(S2\) receives the packet from \(S1\).
5) \(S2\) forwards the packet to the subnet with itself as source address and group address restored to \(G1\).
6) Bob receives the message from \(G1\) finally.

To generalize, each gateway in AoS will join ASM groups within the subnet it serves, as well as SSM groups rooted at other gateways, to receive data from different ASM subnets. Subsequently, it will relay data it received from SSM backbone into its ASM subnet and vice versa.

C. Gateway

Gateway is the key component of the AoS architecture. Therefore, its design is critical to achieve the design requirements. In the following paragraphs, core functionalities of AoS gateway are elaborated in details.

1) Multicast Address Mapping: As ASM and SSM groups are associated with different address spaces, the group address need to be changed during traversing different networks. A stateless, one-to-one mapping would be favored here so that no state is introduced and any gateway can restore and validate the original group address.

For IPv4, ASM is assigned 224.0.2.0/24 through 224.0.255.0/24, while SSM is assigned 232.0.0.0/8 [10]. Thus, any dynamically assigned ASM address could be directly embedded into a SSM address. For example, ASM group 224.0.111.222 has a one-to-one mapping with SSM group 232.0.111.222.

The situation is a bit complex with IPv6, whose multicast address format is defined as Fig. 3 [11]. Non-prefix-based and embedded-RP multicast group addresses are deprecated in AoS, so the flags field is 0x3, and the scope field for inter-domain multicast is 0xe. Hence, the difference of ASM and SSM addresses lies only in the plen and network prefix fields. When mapping an ASM group address into a SSM one, plen and network prefix fields are filled with zero; when mapping in the opposite direction, the prefix of the sender (gateway) is filled into the fields. For example, if a source sends a message to ff3e:20:2001:db8::89ab:cd0ef, it will be mapped into ff3e::89ab:cd0ef by the gateway of its subnet, the original group address will be reconstructed by putting the unicast prefix of the source gateway (i.e. 2001:db8::/32) into the group address again.

2) Group Discovery and Update: In order to forward packets, a gateway should join appropriate ASM and SSM groups when it is initialized and dynamically join and leave them as required. Hence, it needs to acquire information about group discovery and update.

To achieve this, a gateway first needs to know the sources and receivers in its subnet and the multicast group they associate with. To keep the routing infrastructure intact, this could be done with low-layer plug-ins installed on multicast-capable end hosts, which are similar to connection management widely used today. Plug-ins inform gateway when applications on a host join and leave a session or send data towards some multicast group.

Upon a receiver requests to join some multicast group, the corresponding gateway lookups which subnets have source sending data towards this group. Distributed systems, e.g. Distributed Hash Table (DHT) system [12] running among gateways would satisfy such requirement in a scalable way and the burden of flooding information on backbone routers thus is saved.

3) Security and Management: According to the address mapping rules introduced above, packet forwarding could be performed by the gateways without any state stored. Therefore, this stateless packet forwarding is a secure and scalable one.

Gateways are required to record the registration of local sources and receivers, which could be subject to potential Deny-of-Service (DoS) attack. However, the benefit of such registration outweighs its shortcoming in several aspects. First, source registration provides a way for ISP to enhance multicast management in allowing them to authorize and authenticate...
multicast traffic, which further enables admission control and traffic engineering. Second, as each gateway only accepts registration request from local subnet, even if there exists attempt to attack, the source could be easily determined and charged. Finally, register functionality could be located separated from the server performing stateless packet forwarding, which would further reduce the impact of potential security attack.

IV. Evaluation

A serials of evaluations are done to validate the viability of AoS architecture. Throughout the evaluations, we focus on two characteristics: the scalability of AoS and the performance of the gateway. Both aspects are demonstrated in the following paragraphs.

A. Scalability

Simulation is conducted to evaluate the scalability of AoS architecture under large-scale deployment. The network topology used in the simulation is a 54-node-network extracted from an actual ISP’s network, adopted from [13], as illustrated in Fig. 4. The hexagons in the topology stand for core routers in the backbone network, and the ellipses represent the subnets attached to the backbone.

We assume that a number of multicast application users will be randomly distributed in all the subnets, while no user would be directly attached to the core routers. To make it perspicuous, we just simulate the situation with single backbone and single multicast group, though it’s easy to generalize to the situation with multiple backbones and multiple multicast groups.

We control the number of users and the ratio an user could be a source to reflect different multicast applications, and each result below is the average of 5 rounds of simulations with the same parameter set.

1) Comparison with MSDP: In inter-domain ASM with MSDP, a RP within the source’s domain advertises the source and corresponding group information through flood-and-join method. As shown in Fig. 5(a), the result of simulation indicates that the number of such source advertisement messages is close to proportional to the sources’ number in a settled network topology. Thus, MSDP fails to scale when senders for a group increases. On the other hand, although the number of DHT query operations in AoS related to user number when there are a few users (less than 200 in our simulation), it stops to grow up as the number of user further increases, and remain in very small amount regardless the ratio of the senders.

The number of join messages generated during the procedure, as illustrated in Fig. 5(b), characterizes the dynamics of multicast routes in backbone. The join messages in MSDP come from two parts: when a client joins the CBT of \((*,G)\) (assuming RP of backbone network is router 0) and when a client further switches to the SPT of \((S,G)\). The result shows that the number linearly climbs with the growing user number. However, in AoS the join messages are created only when a gateway of a subnet joins a SSM tree \((S,G)\) of another subnet. Difference also exists in that \(S\) for AoS stands for some gateway responsible for the subnet, not the actual source of the multicast group. Hence, the number of join messages is also limited to the scale of the underlying network topology.

2) Comparison with Embedded-RP: The source advertisement method is abandoned in IPv6 multicast, while the RP address is embedded into the multicast group address. This eliminates the message flooding of MSDP, while results in that a RP of some private ISP must be required to serve the clients from other ISP. Besides the security and interest concerns of ISP, the result of our simulation shown in Fig. 6(a) also indicates that the performance of multicast routing would be degraded due to the detour routing: assuming the RP address embedded is RP for the first source of that group, the average route length in hop is two times as long as the one in AoS.

The join procedures with MSDP and Embedded-RP have few differences except that for Embedded-RP the root of CBT is the RP for the first sender, not the RP of core network. Consequently, the result in Fig. 6(b) is similar to that of Fig. 5(b), indicating that AoS also scales better than Embedded-RP in the sense of route dynamics.
B. Performance

A prototype of AoS gateway is implemented and is deployed in China's Next Generation Internet - CERNET2 to have its functionality tested and performance evaluated. Ordinary commercial workstations\(^1\) equipped with the AoS module under GNU/Linux are used, and DVTS\(^2\) is adopted as the application in our evaluation.

We first evaluate CPU and memory usages under single data stream with different data rates, whose result is shown in Fig. 7(a). Even with 90Mbps data rate, the usage of memory is lower than 20\%, and that of CPU is about 10\%. After that, the scenario when multiple ways of data stream with 300Kbps data rate are concurrently served is also evaluated, as illustrated by Fig. 7(b). Packet loss won't appear until there are more than 1500 streams, and there will be a loss rate of 40\% only when the number of streams reaches 3000.

The results of the performance evaluation show that our gateway is capable for forwarding multiple streams with relatively high data rate. This is majorly because that a stateless packet forwarding scheme is used in the AoS architecture, which saves great burden from both CPU and memory of the gateway.

V. Conclusion

It has been a period of time since people started to argue the great burden of routing states and dynamics brought by ASM had been obstructing the deployment of large-scale inter-domain multicast, while lack of intense requirements in SSM-enabled operating systems and applications often made SSM ignored by the ISP. Our approach of building a two-tier inter-domain architecture hereof combines the benefits of both current ASM and SSM. Furthermore, the dynamics and complexity in backbone routers are reduced, and at the same time some security and management features are introduced.

Without modifications on current routing infrastructure and multicast applications, our approach succeeded all features through adding a intermediate gateway into the inter-domain multicast. Evaluations demonstrate that our AoS architecture is indeed scalable in that it mitigates the message propagation as well as routing states in the backbone network, and AoS gateways are capable to forward large quantities of multicast traffic traversing through it.

REFERENCES