Research of Secure Anycast

Zhiguo Zhou
College of Computer Science and Technology
Jilin University
Changchun, P.R. China
College of Computer
Northeast Normal University
Changchun, P.R.China
zhouzg281@nenu.edu.cn

Gaochao Xu
College of Computer Science and Technology
Jilin University
Changchun, P.R. China
xugc@jlu.edu.cn

Jinxin He
College of Computer Science and Technology
Jilin University
Changchun, P.R. China
College of Earth Science
Jilin University
Changchun, P.R.China
he_jinxin@126.com

Chunyan Deng
College of Computer Science and Technology
Jilin University
Changchun, P.R. China
dengcy@jlu.edu.cn

Abstract

Anycast is a new communication mode in the standards of IPV6. A host can communicate with the "nearest" member in the destination group through anycast. Because the group management and the routing protocol in the anycast are not so mature, when communicating it is easy to be utilized by some attacks such as masquerading and denial of service, etc. Utilizing the correlative secure technology of Multicast, we propose a new group management method to secure anycast on the basis of others' research in this paper, which can ensure the security of anycast server and the secure communication between anycast client and server. This method has been proved to be effective.

1. Introduction

With the rapid development of computer technology and the widely use of Internet, more and more users share and access information through WWW. Many popular sites may block because of the excess users. To enhance the usability of service and improve network load, we often use mirrored web server, which means to connect multi servers with same services to each other through network to provide the same service to users together. In Internet we can adopt a new service model-anycast [1] to support the distributed replication of server so as to improve network load, simplify network application and satisfy different users' requirement of QoS [2]. Anycast is a new communication mode, which has been defined as a standard in Ipv6 together with unicast and multicast. Multicast is a communication way from one or more senders to multi receivers, Anycast is from a host to any member of destination group, whereas unicast is a special case of the anycast communication when there is only one member in destination group. Through

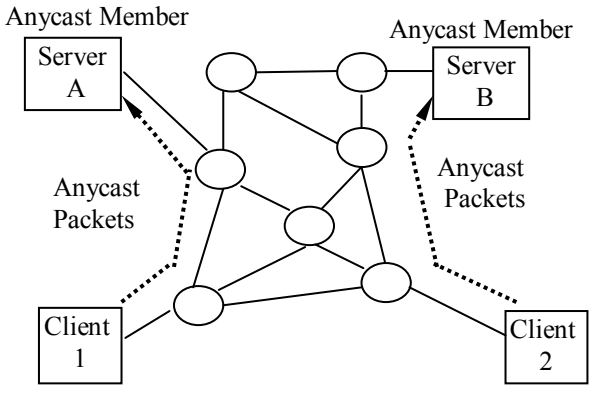

Figure 1. **Anycast model**

This research is supported by Jilin Province Natural Science Foundation of China (Grant No.20050522)

anycast service mechanism, users can receive the service offered by the nearest server to obtain information such as weather reporting and stock quote streaming.

Nowadays anycast technology has developed towards two main directions. One is utilizing the idea of anycast on application layer to implement anycast service and optimize network application [3]. News server is the example. The other is making use of anycast routing technology on network layer to realize anycast service and improve the efficiency of the network communication and robustness. DNS [4] is the example. To a large degree, the implementation of anycast on network layer lies on the selection of routers, so the routing algorithm is very important to the realization of anycast transmission. Presently the study of Anycast on network layer is just underway. Weijia Jia and others have developed the pilot study on anycast routing algorithm [5][6].

The routing protocol defined in current anycast technology standards is not clear, so there are still some technology problems in the application of IPV6.

(1) Scalability. Because of the distribution of the members of anycast, routing items of anycast addresses cannot be assembled. So the routing items of anycast addresses should be saved in the routers separately, and the routing tables will become crowded when anycast addresses are used widely.

(2)Security. Maintaining the membership of anycast is especially important. The simplest way to acquire membership is to broadcast the corresponding routing items of entering routers. But this method sometimes may leads to serious security problems. For example, anycast host could add or delete routing items on routing table freely.

(3) Criterion of selecting membership. Criterions vary with different applications. If rapid response is needed in the application, the transmission delay between source node and anycast node appears very important, so the nearest node of anycast membership need to be selected. Selecting a criterion of anycast routing mechanism affects the capability of anycast transmission greatly.

Because the group management and the routing protocol in the anycast are not so mature, when communicating it is easy to be utilized by some attacks such as masquerading and denial of service, etc. Utilizing the correlative secure technology of multicast, we propose a new group management method to secure anycast on the basis of others' research in this paper, which can ensure the security of anycast server and the secure communication between anycast client and server.

2. Secure group management

There is a strict restriction about anycast addresses in IPv6, which is anycast addresses can only be allocated to routers, not to hosts, in other words, anycast addresses cannot be the source addresses in transmission. IPv6 announces that this restriction will not be canceled until they obtain more experiences and manage to an accordant solution. The most reason of this restriction is because that there exist great hidden security troubles if hosts are permitted to export anycast addresses to host routers. Before a separate and mature anycast routing protocols and a mechanism responding to inform routing system about the anycast members appear, anycast members have to run the routing protocols by themselves in order to join in the routing system. If anycast member is a host, this host will build its route not by router. In order to support host members, a mechanism is needed to inform routing system about the anycast identification of hosts. This is realized by corresponding group management protocols, which are mainly improved on the basis of Multicast group protocols [6][7].

In addition, if any host can inform routing system that it is an anycast server, some vicious hosts may make use of this to offer mendacious information or masquerade as the anycast servers. This will undoubtedly lead to secure problems, so hosts must be authenticated before they inform routing system about their identification of anycast server.

Presently most research are focused on the group management and routing protocols of anycast, whereas the research on secure group management are so limited, which mainly include:

(1)Gothic[8]：a group access control architecture for secure multicast and anycast. There are distinct and significant security vulnerabilities in both the multicast and anycast model including denial of service, theft or service, eavesdropping, and masquerading. Which propose Gothic, a complete architecture for providing group access control. This is complemented by a proposal for a group policy management system that allows the group owner to be authenticated before being allowed to specify the group access rights. This system can be applied to other works that involve group policy. We also propose methods of integrating Gothic with the group key management system and content distribution tree. Gothic, which is a group access control architecture for secure multicast and anycast, proposes using the signed capabilities based on PKI certificates for anycast members to join the routing system. Gothic compares the capability with the access-token proposed in [9], and deems the capability mechanism more secure and scalable. Although Gothic identifies group members by PKI

certificates, yet it does not discuss client verification that is required in anycast group management.

(2)G-CGA[10]：In this method, it is indicated that the main reason why group membership management in IP Multicast and anycast can be abused is that routers cannot determine if a given host is authorized to join a group (this is sometimes referred to as the Proof-of-Membership Problem). Then it proposes a solution for IPv6 based on Group Cryptographically Generated Addresses (G-CGA). Through this method, certain class of DoS attacks can be limited severely. It is fully distributed and does not require any trusted third party or pre-established security association between the routers and the hosts. A defection of the method is that it will lead to severe result if group keys are lost. So changing the group keys timely are needed, which may take some bothers.

There are some defections in these two methods above, so we propose a new secure group management strategy. To ensure the anycast secure, the following should be guaranteed [11]:

(1)Anycast group having not been authenticated cannot be added to the routing system.

(2)Anycast server having not been authenticated cannot be added to the group.

(3)Transmission should be secure while authenticating.

For the first two above, we still adopt PKI certificates [12] as the identification method of anycast Server and the authentication method anycast member, but we set Certificate Authentication Server-CAS so that the tasks of certificate and authentication are separated from routers. It also improves the reliability and security. In addition, when communicating with anycast, we authenticate not only the identification of anycast group but also the members of group. So we can ensure the security and usability of both the group and any member of the group.

For the third, we adopt the IPSec of Ipv6 to guarantee the security of network layer and use SSL on transmission and application layers.

CAS issues a certificate to every group to identify them; it also issues different capabilities to all member of the group. When authenticating, anycast server need to offers its own certificate, so CAS could authenticate whether this server belongs to some specific group member through this certificate, which can avoid some invalid hosts masquerade as anycast Server to deceive other hosts.

Figure 2 shows the authentication course of anycast group requesting for joining in routing system.

In Figure 2, Group is the group manager of anycast; we use a host as the group manager, which responds to manage the anycast Server of its own group. The management mainly includes receiving the join request

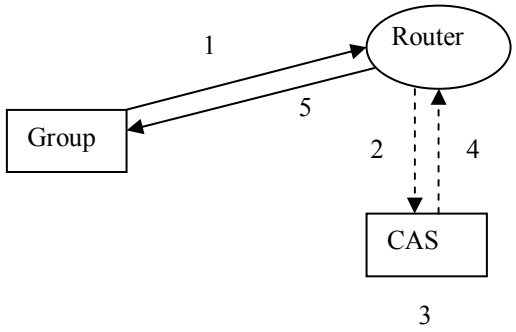

Figure 2. **The authentication course of group**

and the request and validation of being off from hosts, and informing the corresponding routing system about the status of group members. The dashed means different networks.

1.Group manager sends join request to routing system: Join Request with its certificate and unicast address.

2.Routing system sends authentication request to CAS: Authentication Request with its certificate and unicast address.

3.CAS authenticates the request from group manager.

4.Send authentication result to corresponding routing system: Authentication ACK with group's certificate, its unicast address and anycast address.

5.Routing system responds according to the authentication result from CAS: If success, routing system joins this group to the corresponding routing table and responds to the group manager: Join ACK with its unicast and anycast address. If failed, routing system only responds to the group manager: Authentication Failed.

Figure 3 shows the authentication course of any host requesting for joining in the server.

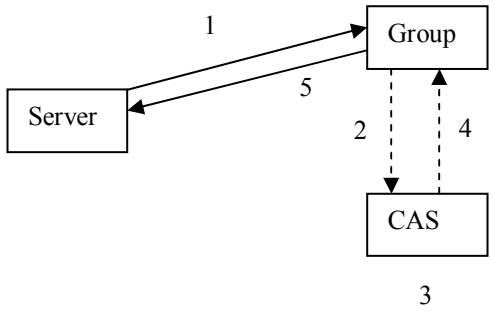

Figure 3. **The authentication course of anycast server**

In Figure 3, Group is the group manager of anycast, Server is any host of requesting for joining in the group, and the dashed means different networks.

1.Host sends join request to group manager: Join Request with its certificate and unicast address.

2.Group manager sends authentication request to CAS: Authentication Request with its certificate and unicast address.

3.CAS authenticates the request from host.

4.Send authentication result to corresponding group manager: Authentication ACK with group's certificate, its unicast address and anycast address.

5.Group manager responds according to the authentication result from CAS: If success, group manager joins this host into the group, announces to the corresponding routing system, and response to the host: Join ACK with its unicast and anycast address. If failed, group manager only responds to the host: Authentication Failed.

3. Secure communication

Because at the beginning of designing IP protocols security is not considered, some enterprises and organization network being attacked and secret data being eavesdropped were often seen at the first time of Internet. To enhance the security of Internet, IETF have taken measures to establish a set of IP Security (IPSec) protocols of protecting IP communication since 1995. IPSec is a part of Ipv6, and it is also a optional extend protocols of Ipv4. IPSec proposes two security architectures: authentication and encryption. Authentication architecture means the data receiver of IP communication can ensure the real identification of the sender and can also judge whether the data has been edited when transmission. Encryption architecture guarantees the confidentiality of data through coding, which can avoid data being eavesdropped and revealed during transmission.

Authentication Header (AH) protocols of IPSec defines the application methods of authentication, and Encapsulating Security Payload (ESP) protocols defines the application of encryption and optional authentication. We can adopt these two protocols or select one of them according to the secure requirement in the application of IP communication. AH and ESP both provide authentication service, but the service provided by AH is more powerful than that by ESP.

When using AH or ESP in a specific IP communication, protocols will associated with a set of security information and service, which is called Security Association (SA). SA may include authentication algorithm, encryption algorithm and key for authentication and encryption. IPSec creates and maintain SA through a key allocating and exchanging protocol, such as Internet Security Association and Key Management Protocol (ISAKMP).SA is a single logic join, in other words, there are two SA during authentication communication between two hosts, one is for sender, the other is for receiver.

IPSec defines two modes of SA: SA of transmission mode and SA of tunnel mode. SA of transmission mode means inserting AH or ESP Header after IP Header (or any optional extensive packet header) and before any high layer protocol (such as TCP and UDP) Header. SA of tunnel mode means placing the whole original IP data packet into a new IP data packet. When SA of tunnel mode is adopted, every IP data packet has two IP Headers, which are outside Header and inside Header. Outside Header specifies the destination address that will deal with IP data packet, and inside Header specifies the final destination address of original IP data packet. SA of transmission mode can only use for the IP communication between two hosts, while SA of tunnel mode can used for IP communication not only between two hosts but also between two security gateways even between a host and a security gateway. Security gateways may be routers, firewalls and VPN devices.

In our anycast model, we adopt the duplicate of IPSec of SA of tunnel mode defined in Ipv6 on network layer to ensure the security, and use SSL protocols, which is perfect in present, during transmission.

4.Evaluation

To evaluate this method, we construct a small network environment, which include two routers (CISCO 2651XM), ten PCs (DELL OPTIPLEX GX2700), three anycast Servers (one for certification and authentication) and five Clients (one for running hacker software, such as masquerading and denial of service)[13]. The experiment shows that those methods mentioned above are all failed. In the contrast experiment, we don't adopt secure group management. The latter experiment reveals that anycast Packets have been lost severely, anycast Server sometimes even cannot be accessed. So our approach is effective and reasonable.

5. Conclusion and Future work

In this paper, we have studied the secure anycast group management architecture based on multicast routing algorithms and protocols and group management protocols in multicast. Through importing the advanced authentication architecture to anycast group management, we implement a secure group management frame. We also construct a secure anycast model under this frame combining IPSec with other security technology. This model is still in the stage of experiment, so some related work should be continued to improve it.

6. References

[1] S.Deering and R.Hinden, “Internet Protocol version 6(IPV6) specification”,RFC 2460,Dec, 1998

[2] Clauio Casetti, Renato Lo Cigno, Marco Mellia, Maurizio M.etc, “A new class of QoS routing strategies based on network graph reduction”, *Computer Network,* 2003,41(4), pp.475-487.

[3] Ellen W. Zegura, Mostafa H. Ammar, Zongming Fei, Samrat Bhattacharjee, “Application-layer anycasting”,In proceedings of the IEEE INFOCOM ’97 (1997)

[4] Sandeep Sarat,Vasileios Pappas,Andreas Terzis, “On the use of anycast in dns”, SIGMETRICS’05,June 6,2005, pp.394-395.

[5] Jia W,Xuan D,Zhao W,“Integrated routing algorithms for anycast messages”,*IEEE Communications Magazine*,January 2000,pp.48-53.

[6] Weijia Jia,Gaochao Xu,Wei Zhao,Pui-On Au, “Efficient internet multicast routing using anycast path selection”,J*ournal of Network and Systems Management*, Vol. 10, No. 4, December 2002,pp.417-438.

[7] Dina Katabi,John Wroclawski, “A framework for scalable global ip-anycast(gia)” SIGCOMM 2001,pp.186-219.

[8] Judge, P. ,Ammar, M. ”Gothic: a group access control architecture for secure multicast and anycast” INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE Volume 3, 2002(3),pp.1547-1556.

[9] A. Ballardie and J. Crowcroft, “Multicast-specific securitythreats and counter-measures”, Proceedings of ISOC Symposium on Network and Distributed System Security,San Diego, California, February 1995.

[10] Claude Castelluccia, Gabriel Montenegro, “Securing Group Management in IPv6 with Cryptographically Generated Addresses”, iscc, Eighth IEEE Symposium on Computers and Communications, 2003,pp.588.

[11] L. Dondeti, T. Hardjono, B. Haberman, “Security Requirements of IPv6 Anycast”, draft-dondeti-ipv6-anycast-security-00.txt, Internet Draft, IETF, June 2001. Work in progress.

[12] T. Hardjono, B. Cain, “Key establishment for IGMP authentication in IP multicast”, IEEE European Conference on Universal Multiservice Networks (ECUMN), CREF, Colmar, France, 2000

[13] Naqvi, Syed Riguidel, Michel, “Secure data exchange between intelligent devices and computing centers”, Proceedings of the SPIE, Volume 5803, 2005,pp.157-166.