

Designing Pastry-based Secure IPTV Video Delivery Network

Hyeokchan Kwon, Yong-Hyuk Moon, Jaehoon Nah, Dongil Seo
Electronics and Telecommunications Research Institute
{hckwon, yhmoon, jhnah, bluesea}@etri.re.kr

Abstract. In this paper, we propose pastry-based secure IPTV video delivery network. Pastry, one of the overlay networks, is very suitable for constructing application level IPTV video delivery network because it has scalable and self-organizing properties. But, there exists several security vulnerabilities of pastry-based IPTV video delivery network. This paper analyzes the security threats of pastry-based IPTV video delivery network and we present pastry-based secure IPTV video delivery network. For this mechanism, we introduce rendezvous point authentication mechanism concept to the pastry-based IPTV video delivery network.

1. Introduction

Currently, Commercial IPTV is mainly serviced on the premium network. Therefore, in case of open IPTV environment, the IPTV video is delivered on public network, in this case network load and management cost is a big issue. For example, personal IPTV broadcaster can't manage IPTV dedicated network. So, recently there is the attempt to use overlay-based multicast to distribute streaming media data to reduce network load and management cost.

Pastry[1], one of the overlay networks, is very suitable for constructing p2p-based IPTV video delivery network because it has scalable and self-organizing properties. [2] proposed the pastry based overlay multicast mechanism. It is very efficient solution, but it doesn't provide security mechanisms for protect overlay multicast network. This mechanism is suitable to non-financial applications not financial application such as IPTV and so on.

In this paper, we analyze the security threats of pastry-based IPTV video delivery network and we present security solutions against it. To do this, we introduce rendezvous point authentication mechanism to the pastry-based IPTV video delivery network. In this scheme, only pre-authenticated node can be a rendezvous point.

The contents organized as follows. Section 2 presents overview of pastry-based video delivery network. And in section 3, we present secure IPTV video delivery network. Finally conclusion is given in section 4.

2. Overview of pastry-based video delivery network

In this section, we provide pastry-based video delivery network.

2.1 Overview of pastry routing

Pastry[1] is one of the DHT(Distributed Hash Table)-based overlay networks. The node ID of pastry is generated by secure hash of the node's public key or IP address. Pastry reliably routes the message to the pastry node with the node ID that is numerically closest to the key. Pastry uses the prefix routing. In the prefix routing, the node forward the messages to a node whose node ID shares longer prefix with the given key comparing the present node, if no such node, forward it to a numerically closer node.

0	-1-1212	-2-2301	-3-1203
1-0111	1-1133	2	1-3022
1	02-110	02-230	02-323
021-00	021-10	021-22	3
0213-0	0213-1	0213-2	3

Figure 1: Pastry routing table example

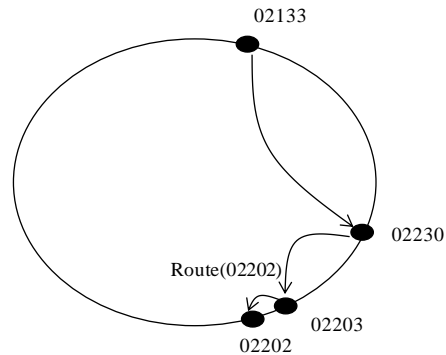


Figure 2: Pastry routing table example

The node IDs and keys are thought as a sequence of digits with base 2b. The tables required in each Pastry node have only $(2^b - 1) * \lceil \log_{2^b} N \rceil + 1$ entries. L is a number of entries in Leaf set. A node's routing table organized into $\lceil \log_{2^b} N \rceil$ rows with base 2b -1 entries each. The $2^b - 1$ entry in row n of the routing table each refer to a node whose nodeId matches the present node's nodeId in the first n digits. Figure 1 shows the pastry routing table examples. For example node 02133 whose routing table is shown in figure1 routes message 02202 to node 02230. Figure 2 shows this routing example.

2.2 Overview of pastry-based IPTV video delivery network

In this subsection, we introduce pastry-based video delivery network. The target network is SCRIBE overlay multicast network, which is build on top of pastry. SCRIBE[1] is a large-scale, decentralized application level multicast infrastructure built upon pastry[2], a scalable, self-organizing peer-to-peer object location and routing substrate overlayed on the Internet. There exist 4 types of API that is used by SCRIBE[1]. (1) create(credentials, groupId) (2) join(credentials, groupId, messageHandler) (3) leave(credentials, groupId) (4) multicast(credentials, groupId, message)

Each group of SCRIBE has a unique groupId. The group id is generated by hash of group's name and creator's name. The figure 3 and 4 shows the process of group creation and Join.

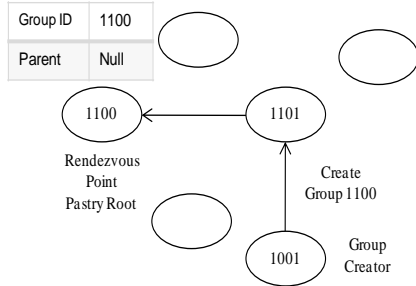


Figure 3 The process of Group Creation

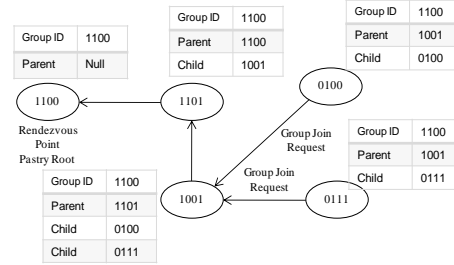


Figure 4 The process of group Join

In figure 3, peer 1001 send the group creation message to node 1100(1100 is the groupID), and message is routed to node 1100. In figure 3, the group creation message is routed through the node 1101. This routing path is decided by prefix-based pastry routing table for each node. Each peer in this route can be a member of this multicast tree automatically. These peers store the information of parent peer and child peer during the deliver creation message. In this case the node 1100 is the rendezvous point of the group. rendezvous point is a root of multicast tree. Figure 4 shows the process of group join. In figure 4 node 0111 join request to group 1100. Figure 5 shows the overlay multicast tree after the creation and join group. The node 1100 in figure 5 is pastry root and rendezvous point.

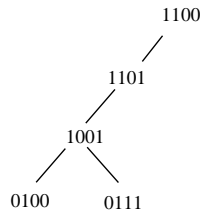


Figure 5 Overlay multicast tree

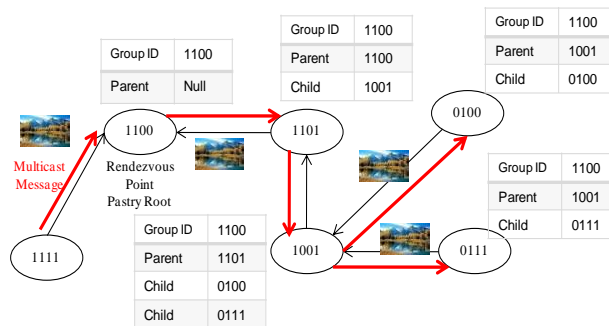


Figure 6 The process of IPTV video delivery

Figure 6 shows the multicast routing process. The node 1111 request message multicast to the rendezvous point of the group (node 1100), and the message is multicast to the group members

through the multicast tree. In case of overlay-based IPTV service, the group (ID: 1100) can be a channel and the members of the group can be a viewer of that channel and the node 1111 is a content provider of that channel.

3. Secure IPTV video delivery-network

3.1 Security vulnerability of pastry-based video delivery network

In this subsection, we analyze security threats of pastry-based video delivery network - SCRIBE. In this architecture, the peers in which there is no access right of media but in the pastry transmission path can be a member of a multicast tree. So it is needed to protect multicast media data from these unauthorized members. Moreover because the arbitrarily selected peer can be operates as rendezvous point, the security threat by malicious rendezvous point exists. In this case a multicast is almost impossible in case that malicious peer plays the role of rendezvous point. For example, a set of malicious nodes can make malicious rendezvous point. And they forward the join message from a new node to a malicious rendezvous point. Moreover, it is possible that a malicious node could forward multicast data to an incorrect node or drop it. Because, it is not possible to verify the multicasting routing is done successfully or not.

Therefore, Information leakage is possible vulnerability. In SCRIBE architecture, Some members of the multicast tree have no right for seeing multicast data. These members only perform pastry routing. These member could sniff, store, re-distributes the multicast data illegally.

Therefore DoS(Denial of Service) attack is also possible when a set of malicious node forwards the multicast data to a specific target node cooperatively. On the other hand, stream pollution and forgery routing message attack is also possible. In this attack, The attacker mixes into the stream bogus chunks, which degrade the quality of the rendered media at the receivers[3]. Therefore, an intermediate node can forges and delivers the routing messages. Particularly, the routing system can be collapsed in case of forging the control message.

3.2 Security architecture

In this subsection, we propose brief solutions against security vulnerability of pastry-based video delivery network. And we present pastry-based secure video delivery network.

To protect from malicious rendezvous point, we introduce the mechanism to authenticate rendezvous point. To do this pre-select the nodes that can be a rendezvous point and send rendezvous point certificate to them. The rendezvous point can be decided to numerically closest to groupID from rendezvous point candidate nodes. To protect from information leakage, it is possible to introduce group key management functions to rendezvous point. The rendezvous point issues the group certificate for group member, and delivers it to the group member directly not using pastry routing. The rendezvous point encrypts the media data by using group key. To protect from disturb multicast routing it is possible to introduce the functions of monitor delivery status of multicast data to rendezvous point, and apply incentive mechanism. Otherwise reputation based trust management

system is also possible solution. To protect from DoS attack, it is possible to introduce the functions of monitor delivery status of multicast data to a rendezvous point, and apply incentive mechanism to the system. And stream pollution and forgery routing message attacks can be protected by using stream encryption, hashing of control message and so on.

From now on, we describe detailed mechanism for secure IPTV media delivery network. For this mechanism, we introduce the rendezvous point manager(Rm) and rendezvous point candidate(Rpc) The system component is shown in figure 6.

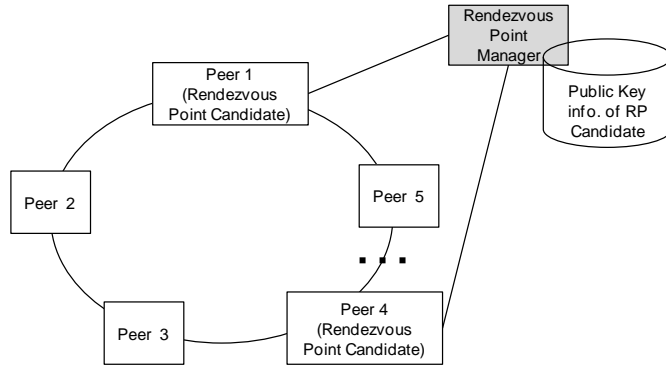


Figure 6 Service component

The rendezvous point manager(Rm) manages rendezvous point candidate. We assume that Rm knows the node id and public key of rendezvous point candidate in advance. rendezvous point candidate is pre-selected by the system and the rendezvous point is selected to numerically closest to groupID from RP candidates. In this application, we assume that each pastry node knows the public key of Rm by downloading the application software with root certificates of Rm as part of the binary. In our approach, each node self-generates public/private key pairs. Rm is not a certificate authority server in public key infrastructure, it only manages rendezvous poin candidates and provides the information of RP candidate.

Table 1 shows the notations to be used in this paper.

Table 1. Notations

Notation	Meaning
Rp	Rendezvous Point
Rm	Rendezvous Point manager
K_k^u	Public key of peer k
K_k^r	Private key of peer k
$E_k(m)$	Encryption function. Encrypt the message m by encrypt key k
$D_k(c)$	Decryption function. Decrypt the cipher text c by decrypt key k
$S_k(m)$	Signature function. Signing to message m by key k

■ **The process of group creation**

As follows is the detailed scenarios of group creation – Node D6A creates group D45. In this scenario, the node D49 is rendezvous point candidate node.

Phase 1) D6A → D43

- D6A Generates group creation message and send it to the pastry network.
- The message is delivered to D43 by pastry routing

Phase 2) D43 → D45

- D43 update its multicast table(its parent node is D45 and child node is D6A and send the message to D45 by pastry routing

Phase 3) D45 → D49

- D45 is not rendezvous point candidate, so D45 searches rendezvous point candidate node from its routing table. And send the message to D49 which is rendezvous point candidate, and update its multicast table.

Phase 4) D49 → D6A

- D49 send the new group ID signed by its private key to the group creator D49 .

$$\{\text{newGroupID}(D49)\} | S_{K_{D49}^r}(m) \quad (1)$$

Phase 5) D6A → Rp manager

- D6A requests D49's public key to the Rp manager. The message is encrypted by Rp's public key

$$E_{K_{Rm}^u}(\text{"Request public key of Rp}(D49)\text{"}) \quad (2)$$

Phase 6) D6A → Rp manager

- Rm decrypt the message by its private key, and send the public key of D45. The message is signed by Rm's private key.

$$\{K_{D49}^u\} | S_{K_{Rm}^r}(m) \quad (3)$$

Phase 7) D6A → D49(Rp)

- D6A verify the signature of Rm using Rm's public, and get D49's public key from this message and verify D49's signature of equation 1 in phase 4.
- D6A send the create group message to D49. The message is encrypted by D49's public key.

$$E_{K_{D49}^u}(ID_{D6A} | K_{D6A}^u | \text{"create group D49"}) \quad (4)$$

Phase 8) D49(Rp) → D6A

- D49 decrypt the message by its private key and return group creation success message and group key to D6A.

$$E_{K_{D6A}^u}(\text{"success group creation"} | K_{D49}^g) \quad (5)$$

Phase 9) D6A

- Get Group key from the message in phase 8

■ **The process of group join**

As follows is the detailed scenario of group join – Node D6E joins the group D49.

Phase 1) D6E → D43 → D45 → D49

- D6E generates join group(D49) request and send it to the pastry network.
- The message is delivered to D49 by pastry routing through D43, D45 node.
- The D43 and D45 update its multicast table before the forward joins.

Phase 2) D49(Rp) → D6E

- D49 request public key of D6E, the message is signed by private key of D49.

$$\{\text{"request public key of D6E"}\} \mid S_{K_{D49}^r}(m) \quad (6)$$

Phase 3) D6E → Rm, Rm→D6E

- D6E request the public key of D49 to Rm(equation 7), and then Rm send public key of D49 to D6E (equation 8)

$$E_{K_{Rm}^u}(\text{"Request public key of RP(D49)"}) \quad (7)$$

$$\{K_{D49}^u\} \mid S_{K_{Rm}^r}(m) \quad (8)$$

Phase 4) D6E → D49

- D6E send its self-generated public key to D49

$$E_{K_{D49}^u}(ID_{D6E} \mid K_{D6E}^u \mid \text{"join group(D49)"}) \quad (9)$$

Phase 5) D49 → D6E

- D49 send the group key to D49

$$E_{K_{D6A}^u}(\text{"success group join"} \mid K_{D49}^g) \quad (10)$$

Phase 6) D6E

- Get Group key from the message of equation 10 in phase 5

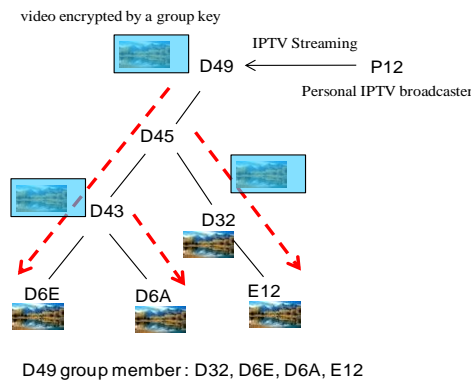


Figure 7 The process of IPTV video delivery

The figure 7 shows the process of IPTV video delivery. This mechanism can protect IPTV video delivery network from the malicious rendezvous point, because it can provide the mechanism to authenticate rendezvous point candidate. And this mechanism can protect information leakage, because it introduces group management functions to the authorized rendezvous point and the multicast video data is encrypted by group key which is generated by rendezvous point.

4. Conclusions

In this paper, we analyze the security threats of pastry-based IPTV video delivery network and we present security solutions against it. To do this, we introduce the rendezvous point authentication mechanism to the pastry-based IPTV video delivery network. In this mechanism, only pre-authenticated node can be a rendezvous point.

This mechanism can't solve overall security threats of overlay-based IPTV video delivering, but it can provide security solutions against malicious rendezvous point in overlay-based IPTV video delivery network. The proposed mechanism is very simple, easy to implement and low cost mechanism in comparison to public key infrastructure and so on. And it doesn't interfere with the operation of traditional overlay based IPTV delivery network like pastry and so on. In the future work, we will extend the mechanism to consider various service scenarios and security threats such as denial-of-service attack and so on.

Acknowledgement

This work was supported by the IT R&D program of MKE/KCC/IITA [2008-S-006-01, Development of Open-IPTV (IPTV2.0) Technologies for Wired and Wireless Networks].

References

- [1] A. Rowstron and P. Druschel, "Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems," *Proc. of the 18th IFIP/ACM Int'l Conf. on Distributed Systems Platforms* (Middleware 2001). Heidelberg, Germany, Nov. 2001
- [2] M. Castro, P. Druschel, A. Kermarrec, and A. Rowstron, SCRIBE: A large-scale and decentralized application-level multicast infrastructure, *IEEE Journal on Selected Areas in Communications*, Vol.20, No.8, Oct 2002
- [3] T. Qiu, I. Nikolaidis and Fulu. Li, On the Design of Incentive-Aware P2P Streaming, *Journal of Internet Engineering*, vol. 1, no. 2, Oct. 2007
- [4] Stephanos Androutsellis-Theotokis and Diomidis Spinellis, "A survey of peer-to-peer content distribution technologies", *ACM Computing Surveys*, 36(4):335–371, December 2004