

Method for providing reliable peer activity report for managed P2P communications

Wook Hyun*, JuYoung Park*

* ETRI (Electronics and Telecommunications Research Institute), Korea

whyun@etri.re.kr, jypark@etri.re.kr

Abstract— In P2P-based contents distribution, an overlay network is constructed by peers that reside in user domain not service provider domain, and each peer shares data with each other. Due to the unmanageability characteristics of P2P networking, it tends to lead to inefficiency due to ignorance of underlying network in spite of its advantages and unfairness caused by absence of incentives to contributing peers. In order to solve several issues regarding P2P networking and making use of its advantages compared to existing server-client model, ITU-T Q.9/11 is developing a series of MP2P (Managed P2P communications) standards. In order to figure out the status of overlay network and gathering activities information of peers, it aggregates the information from peers that may not be trusted due to the possibility of forgery. It is important to assure the integrity and non-forgery of reports from peers. In this paper, we propose a method for gathering reliable peer activity report by use of digital signatures.

Keywords— P2P, peer activity management, PAMP, reliable report

I. INTRODUCTION

P2P-based contents distribution method provides more enhanced performance and scalability compared to server-client model since each data is exchanged among peers. This approach unburden the cost of service providers, but it leads to increase of inter-domain traffic that may burden ISP in aspect of revenue as well as traffic management issues. As well as inter-domain traffic and flash crowd, P2P is used for illegal distribution of copyrighted contents. In order to issue these problems, ISO/IEC has developed a framework for managed P2P communications^[1] as shown in Figure 1. ITU-T SG11 Question 9 is under development a series of MP2P Recommendations^{[2][3]} for providing management features to P2P overlay networking. Especially, it is important to know the status of overlay network as well as cooperation with ISP that provides underlying physical networks. In managed P2P networking, it gathers status information of peers in order to figure out the status of overlay network.

In order to gather the information from peers, ITU-T X.mp2p-pamp (Peer activity management protocol)^[3] is under development that provides a mechanism to gather peer's status and activity information. This gathered information can be used for providing incentives or charging based on the activity within an overlay network.

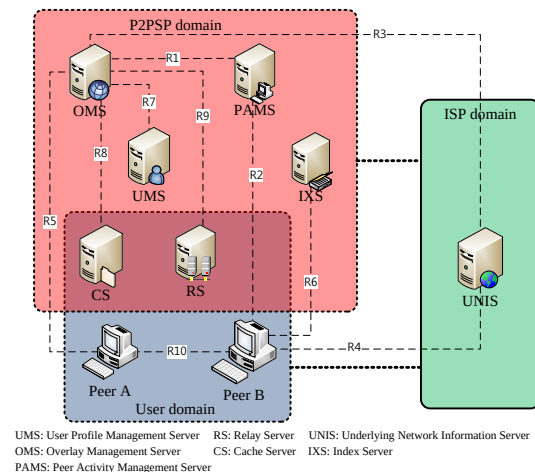


Figure 1. Overview of managed P2P networking architecture^[1]

By the way, since the information is gathered from peers, it needs to provide a method for confirm whether the report is correct or not. In this paper, we propose a method for providing reliability on report received from peers by use of digital signature.

II. RELATED WORKS

There are several related works regarding incentives mechanisms in P2P networking.

Piatek *et al.*^[4] abstracts design and implementation of *Contract* that provides contribution incentives in P2P live streaming systems. This *Contract* scheme rewards each peer according to its global effectiveness, and it rewards peer's contribution with QoS by effecting the overlay network. In this approach, a service provider makes a level of service that is proportional to the peer's ability in terms of distribution of sliced contents, rather than bilateral reciprocation. It also introduces a method for verifying contributions that includes distributed verifications that broadcasting receipts to all connected peers, and centralized verifications that tacker server receives all messages for verifications. This paper examined performance by deploying on PPLive services.

M. Haridasan *et al*^[5] proposed and evaluated a method for enforcing fairness in a live streaming by use of scalable auditing-based technique. The auditing node finds out selfish

nodes that does not contribute their resources enough. In this approach, each peer runs a local auditors to gather all accountable information regarding data exchanges.

W.Hyun *et al* [6] has proposed a method that makes use of DHT (Distributed hash table)-based overlay networking among PAMS as shown in Figure 2.

Peer activity information is generated by all peers by specific events such as exchanges of sliced piece of contents, or failure of peer interactions. However, if a server aggregates those information at the same time, it may lead to bottleneck that may cause loss of report from peers.

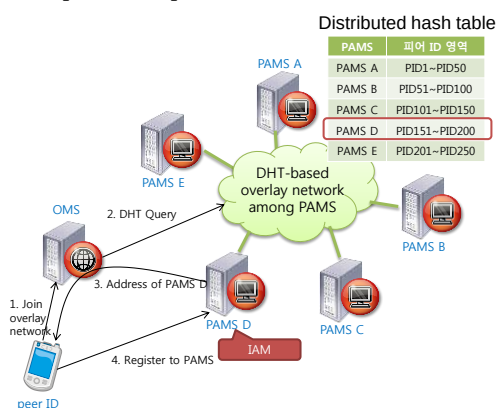


Figure 2. PAMS discovery using DHT[4]

This paper assumes that several servers are distributed over P2P networks. On a peer discovering PAMS that aggregates information peers, it sends DHT query to a special overlay network that consists of PAM servers on joining a particular overlay network. If a PAMS detects the request message, it responds to the requests for registration of the peer.

III. PROCEDURES FOR RELIABLE PEER REPORT

In this clause, we describe a method for reliable report on peer activity message. Figure 3 shows an overall procedures of the method.

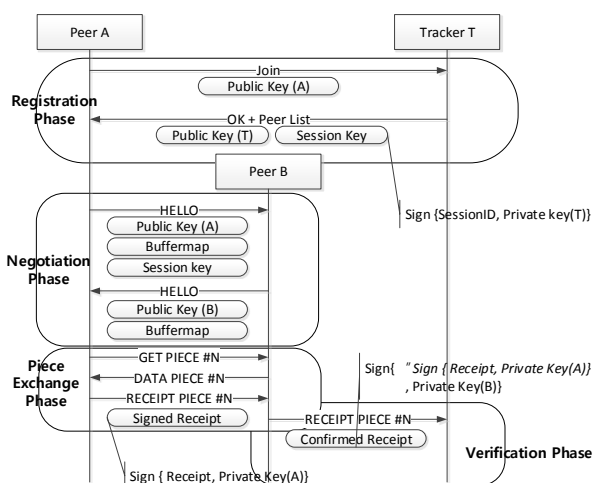


Figure 3. Overall predures for reliable peer report

It roughly consists of four phases; registration, peer negotiations, piece exchange and verification. In this clause we describe each phase with details.

A. Registration phase

When a peer joins to a particular overlay network, it firstly sends registration (or join) message to overlay management server (aka. tracker server). On registering, newly joining peer sends its public key to the server, and the server also return its public key on success registration as well as session key. The session key is used for verify whether the peer has rights to access and receive contents from other peer.

The digital signature from peer is used for verifying the integrity of received report. If the registration is successful, tracker server sends its public key and session key that are used for verifying or decrypting message. Especially, the session key is used for checking session's validity. For example, some session can be expired for streaming service users. In order to prevent from forgery on the session key, this key is signed by private key of tracker server.

Figure 4 shows operation flows of tracker server. When a server receives join request from a remote peer, it firstly check the validation of the user and its public key. If it decides the request is valid, it sends session key and public key of tracker server as well as *peer list* of the overlay network. It is also possible to provide a policy that describes configured actions for the overlay network.

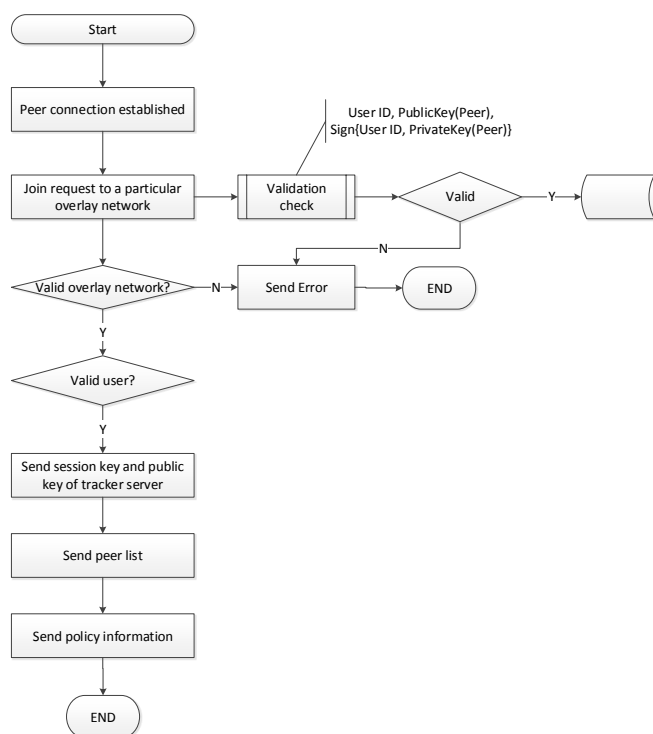


Figure 4. Flows of tracker server for exchanging digital signature and session key for reliable peer report

B. Peer negotiation phase

When a peer negotiates with other peer, both peers exchange their public key as well as *buffermap* that represents the possession status on specific numbered-slices of contents. These exchanged public key are used for verifying receipt message received from with other.

C. Piece exchange phase

After *buffermap* negotiations, each peer requests pieces that it does not have. On receiving the request, a corresponding peer sends the piece (numbered-slice of contents). On successful reception of the requested piece, a requesting peer generates a receipt message and envelope the message with its private key.

Sign {Receipt, Private Key (Requesting peer)}

The receipt message contains followings, but not limited to;

- piece id
- peer id (or network address)
- session key
- timestamp
- average transmission speed
- completion time of piece transmission

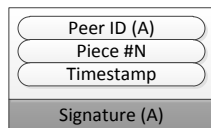


Figure 5. Signed receipt from requesting peer

Figure 5 shows an example of signed receipt message. If a requesting peer does not send the receipt message within a specific time, the corresponding peer may disconnect the relationship with it. This depends on the configuration of the peer. On receiving enveloped receipt message from requesting peer, the corresponding peer verify the message by use of requesting peer's private key that has been acquired during peer negotiation phase.

*Verify {“Sign {Receipt, Private Key (Requesting peer)}”,
Public Key (Requesting peer)}*

When the enveloped receipt is verified, the corresponding peer doubly envelope the receipt by use of its private key.

*Sign {“Sign {Receipt, Private Key (Requesting peer)}”,
Private Key (Corresponding peer)}*

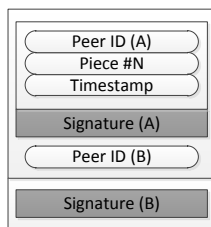


Figure 6. Double-signed receipt from corresponding peer

Figure 6 shows an example of double-signed receipt message made by corresponding peer. The corresponding peer sends the doubly signed/enveloped message to tracker server (or PAMS in MP2P conceptual model).

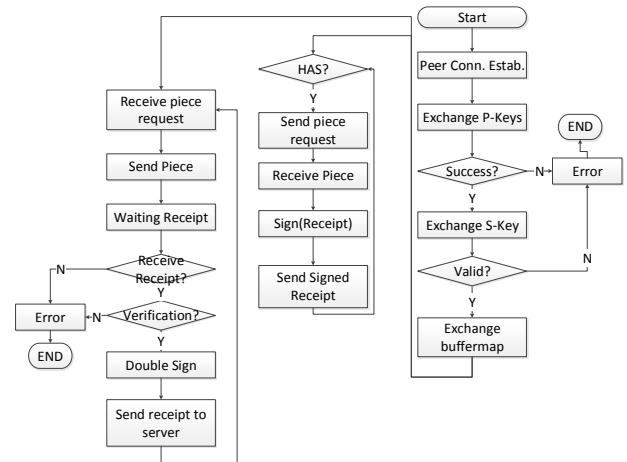


Figure 7. Flows of peer for reliable peer report

Figure 7 shows flows of peer's operation. Since peer acts as client and server at the same time, it has two main flows for interacting with other peers.

D. Verification phase

On receiving doubly signed receipt message from a peer, the server verifies the message with public keys of relevant peers. It use peer identifiers that are embedded within the message.

*Verify {“Verify {“Sign {Receipt, Private Key (Requesting peer)}”,
Public Key (Requesting peer)}”,
Public Key (Corresponding peer)}*

Since the double-signed messages are confirmed by both requesting and corresponding peer, this message can be trusted. On verifying the double-signed message, it makes use of public keys of peers that has been acquired during registration phase. Also, since the receipt message contains identifiers of peer, it is able to find appropriate digital signature for verification.

IV. CONCLUSIONS

Nowadays, the size of multimedia contents are increasing according to its quality. Especially, when it comes to distribute 4K (or higher) resolution video contents, it needs to consider how to deliver the massive volume of data to massive number of users concurrently. The server-client model does not accommodate the volume of contents and receives. Hence, P2P-based distribution methods will be one of candidates of content delivery. However, this method makes use of user's resources such as network, storage, computing power, it is important to encourage peers to contribute their resources by providing incentives, and figure out the status of overlay network.

In this paper, we have presented a method for assuring reliability of aggregated peer’s activity information from peers by use of digital signatures. Each peer exchanges receipt message that is signed by their own digital signatures after sending/receiving a sliced piece of contents in order to prevent forgery of receipt, and the double signed receipts are verified in service providers. P2P-based contents distribution services such as live streaming and file distributing, it is important to give concrete incentives to the contributing peers, and figure out the status of overlay network for providing robust services.

ACKNOWLEDGMENT

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.R0127-15-1053, Development of standards for distributed UHD streaming protocol).

REFERENCES

[1] ISO/IEC TR 20002, “Managed P2P: Framework”, Dec 2013.
 [2] ITU-T SG11 Recommendation X.609, “Managed P2P: Functional architecture”, June 2015.

[3] ITU-T SG11 draft Recommendation X.mp2p-pamp, “Managed P2P: Peer activity management protocol”, Nov 2014.
 [4] Piatek, M.,Krishnamurthy, A., Venkataramani, A.,Yang, Y.R., Zhang, D., Jaffe, A. ”Contracts: practical contribution incentives for P2P live streaming”, NSDI 2010.
 [5] M. Haridasan, I. Jansch-Porto, and R. van Renesse. “Enforcing fairness in a live-streaming system” MMCN, 2008.
 [6] W.Hyun et.al, “An information sharing method among distributed peer activity management server on managing peer’s activities in MP2P network”, ICACT 2013.



Wook Hyun is a research staff member with ETRI (Electronics and Telecommunications Research Institutes) since 2000. He has received M.S. degree in Information Communication Engineering from Chungnam National University, Korea in 2000. His research interests include VoIP, SIP, NGN, P2P, overlay networking and digital signage.



Ju Young Park is working for ETRI from when he has received his PH.D degree in 2001 from Chungnam National University. Thereafter, he took project editorships both in ITU-T and ISO/IEC/JTC1, and he also has developed three International Standards (IS). His major research areas are smart work, Multicast, QoS protocol and architecture. He also has great concerns on mobile communication and IOT.