# Proposal of a content access control scheme on a reputation value over P2P networks

Kentaro ABURADA[†], Mirang PARK*, Masami IKEDA[‡], Hisaaki YAMABA[‡]and Naonobu OKAZAKI[‡]

[†]Oita National College of Technology, * Kanagawa Institute of Technology, [‡]University of Miyazaki

## ABSTRACT

In recent years, with the improvement of the high speed communication infrastructure, P2P content distribution systems have been attracting more attention. In a P2P content distribution system, the lack of a central management server provides the system its robustness. However, it also leads to problems in content reliability and accessibility. We propose a secure content distribution system with improved accessibility by introducing a secret sharing scheme.

## 1 INTRODUCTION

Client–server systems reach their performance limits if the number of client nodes is increased approach a performance limit as the number of client nodes is increased . On the other hand, a P2P system can continue to perform smoothly as nodes are added, provided that communication bandwidth is sufficient. However, a P2P content distribution system, because of the lack of a central management server, has problems in terms of the reliability of the distributed content. For example, a malicious node can easily distribute fake content or content containing a virus program.

## 2 RELATED WORKS

Palomar's method of implementing an access control scheme generates a content certificate based on a multi-signature to obtain protection of content and access control that depends on the collaboration of only a few nodes[1].

In this scheme, the problem remains of how to set the criteria of the selection of a reliable node among the anonymity of a P2P environment. And, if the owner exited the system, content accessibility becomes a problem because the decryption key cannot be obtained.

### 2.1 Trust management system

A P2P content distribution system requires a high reliability to avoid malicious content. The reputation-based trust management system[2] is best for constructing a trust model in a P2P environment because it creates a rating based on reputations reported by multiple sources.

### 2.2 (k,n) threshold scheme

The (k,n) threshold scheme is a secret sharing scheme proposed independently by Blakley[3] and Shamir[4]. In this scheme, secret information is divided into $n$ pieces in such a way that it is easily reconstructible from any $k$ pieces, but is not reconstructible from any $k-1$ pieces. In addition, this scheme has the advantage that the secret information as cannot be easily guessed.

## 3 Proposed system

In this paper, we implement a reputation-based trust management system with accessibility by the introduction of secret sharing scheme.

This system consists of four procedure,
(i) The content owner selects reliable nodes which then collaborate to generate a content certificate based on reputation. The owner generates the content certificate according to a multi-signature created by the selected reliable nodes. Then, (ii) content is encrypted using a common-key cryptosystem. The decryption key is distributed on the network according to a secret sharing scheme. (iii) A request node requests an access certificate from the content owner. The owner decides whether to generate an access certificate; a generated access certificate includes information on the decryption key. (iv) The request node obtains a decryption key using the access certificate and accesses content. Normally, a user which has an access certificate can access content even when the content owner is disconnected from the system.

Reputation rises and falls according to past actions. If content is distributed, it is important that content transactions take place normally. Frequent failure of content transactions has an significant impact on content distribution. If a node receives malicious content in the form of falsified or virus-infected content, the request node decreases the reputation of the providing node.

## 4 Evaluation

We evaluate the integrity of content, which can get normal content when nodes requested content. Accordingly, we consider the attack types of malicious nodes and evaluate the integrity of content. The type of attackers in the simulation are,

(1) Malicious node responds to every query with a fake data.

(2) Malicious node acts like a reliable node, but it tries to send a fake data when it gets enough reputation.

(3) Malicious node sends normally data to some nodes, but sends fake data to others.

(4) Malicious node sends normally data, but occasionally send fake data.

Table 1: Simulation environment.

| Network model | BA model |
|---|---|
| number of node | 1000 |
| maximum number of node | 1100 |
| minimum number of node | 900 |
| number of distinct files | 100 |
| ratio of malicious nodes | 10% |
| number of divided decryption key $n$ | 20 |
| threshold $k$ | 18 |

(5) Malicious node sends fake data and responds fake reputation when reputation of other malicious node requested.

Simulation environments are shown in Table 1. Network model applies BA model which is an algorithm for generating random scale-free network. In this simulation, firstly, we construct network using BA model. Also, nodes have randomly incidence of entry and exit. At this time, nodes cannot entry such as exceed maximum node number and cannot exit such as fall below minimum node number. Also, owner cannot exit.

When request node finished transaction to collect contents and decryption key, downloads are success if it can decrypt the content. Also, downloads are failure if it cannot decrypt the content because of collected data includes fake data by a malicious node.

## 4.1 Result and consideration

Results of our simulation are shown in Figure 1-3. The x-axis of the figure shows the number of downloads. The y-axis of the figure shows ratio of failure to all downloads. Low ratio of failure to all downloads means each nodes download normally contents, therefore, it assures the integrity of content.

At attack type (1), (3) and (5), most downloads were failure from the beginning. This is due to receiving fake data from malicious nodes because they cannot collect reputation at beginning. However, in the proposed method, ratio of failure to all downloads is rapidly decrease if numbers of downloads are increased. On the other hand, in the existing method, ratio of failure to all downloads is almost constant rate. In the proposed method, nodes can control fake data in the early stage because the nodes collect reputation on all the reliable nodes.

Also, at attack type (2), most downloads were failure from the beginning in the proposed method. Then ratio of failure to all downloads is rapidly decrease if the number of downloads is increased. On the other hand, in the existing method, ratio of failure is slowly increased. In the proposed method, malicious nodes get reputation in the early stage because reputation value is frequently updated, therefore, request nodes receive fake data from malicious nodes.

At attack type (4), ratio of failure is comparable range in both methods when malicious nodes start to send fake data. However, in the proposed method, ratio of failure is decreased in the early stage than the existing method. This is due to controlling fake data from malicious nodes because nodes collect reputation on all the reliable nodes as in the case of other attack types.

From these results, the proposed method assures the integrity of contents than the existing method. We will evaluate the accessibility for the future work.

## REFERENCES


[1] Esther Palomar, Juan M.E. Tapiador, Julio C. Hernandez-Castro, Arturo Ribagorda,"Secure content access and replication in P2P networks", Computer Communications 31,pp.266-279(2008).

[2] A. A. Selcuk, Ersin Uzun, M. R. Parriente, "A Reputation-Based Trust Management System for P2P Networks", IEEE/ACM International Symposium on Cluster Computing and the Grid CCGrid, pp.251-258(2004).

[3] Blakley, G. R.,"Safeguarding cryptographic keys", Proceedings of the National Computer Conference 48, pp.313-317(1979).

[4] A.Samir, "How to Share a Secret", communication of the ACM, Vol.22, No.11, pp.612-613(1979).


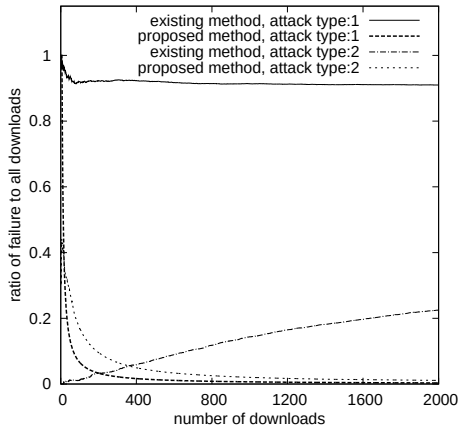


Figure 1: Results, attack type:(1),(2).

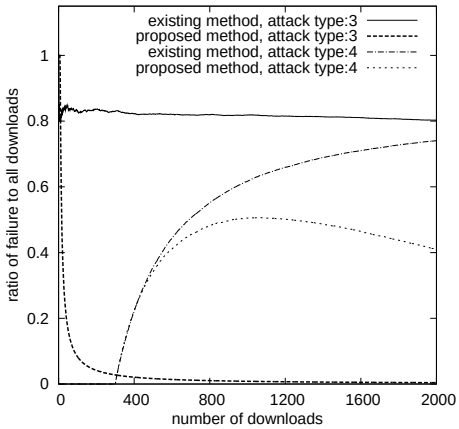


Figure 2: Results, attack type: (3),(4).

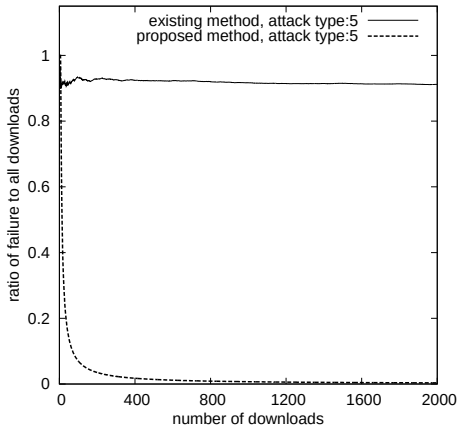


Figure 3: Results, attack type: (5).