THUP: A P2P Network Robust to Churn and DoS Attack based on Bimodal Degree Distribution

Citation:

Katsuya Suto, Hiroki Nishiyama, Nei Kato, Takayuki Nakachi, Tatsuya Fujii and Atsushi Takahara, "THUP: A P2P Network Robust to Churn and DoS Attack based on Bimodal Degree Distribution," IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 247-256, Sep. 2013.

URL:

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6560031

THUP: A P2P Network Robust to Churn and DoS Attack based on Bimodal Degree Distribution

Katsuya Suto, *Student Member, IEEE,* Hiroki Nishiyama, *Member, IEEE,* Nei Kato, *Senior Member, IEEE,* Takayuki Nakachi, *Member, IEEE,* Tatsuya Fujii, *Member, IEEE,* and Atsushi Takahara, *Member, IEEE*

***Abstract*—Hierarchical unstructured peer-to-peer (P2P) networks for file sharing systems such as Gnutella and Kazaa have made a tremendous achievement in the last decade. However, while these P2P networks can be tolerant of churn, i.e., the dynamics of peer participation and departure (or fault), there still remains the issue of vulnerability to Denial of Service (DoS) attacks, i.e., the highest degree peers are removed. In this paper, the failures are modeled in terms of removal of peers from the network to assess the stability of hierarchical unstructured P2P networks. In order to overcome this shortcoming of these P2P networks, we propose a bimodal network based on bimodal degree distribution which is tolerant to both churn and DoS, and an optimal topology. Our proposed scheme, dubbed THUP (churn/DoS Tolerant, Hierarchical, Unstructured, P2P network). Furthermore, we present the most suitable peer joining procedure in THUP. Performance evaluation conducted through computer simulations show that THUP substantially improves the stability and communication efficiency compared with other existing P2P networking approaches.**

***Index Terms*—Bimodal degree distribution, churn and DoS tolerance, hierarchical unstructured P2P networks, neighbor selection.**

I. Introduction

Unstructured peer-to-peer (P2P) networks have been becoming the medium of choice for file sharing systems since Napster and Gnutella [1]. Compared with the centralized P2P networks (e.g., Napster), the original Gnutella network employs a fully decentralized architecture and has attracted much attention because peers can freely participate in the network and depart from the network [2]. However, the original Gnutella network has limited scalability due to its flat topology and flood-based search scheme. As the number of Internet users grows, the advancement of scalability in the Gnutella network is required. To achieve higher scalability, the modern Gnutella network employs a two-tier structure by classifying peers into two subsets; namely ultra peers and leaf peers, as demonstrated in Fig. 1(a). While a few ultra peers behave in the same way as the peers in the original Gnutella network, a number of leaf peers communicate with the other peers through ultra peers. Thus, the modern Gnutella network has become a hierarchical structure, which is an approach employed by super-peer based P2P networks, such as Kazaa and Winny [3], [4].

K. Suto, H. Nishiyama, and N. Kato are members of the Graduate School of Information Sciences at Tohoku University, Japan. (e-mail: suto@it.ecei.tohoku.ac.jp; bigtree@it.ecei.tohoku.ac.jp; kato@it.ecei.tohoku.ac.jp).

T. Nakachi , T. Fujii, and A. Takahara works for NTT Network Innovation Laboratories, Japan. (e-mail: nakachi.takayuki@lab.ntt.co.jp; fujii.tatsuya@lab.ntt.co.jp; takahara.atsushi@lab.ntt.co.jp).

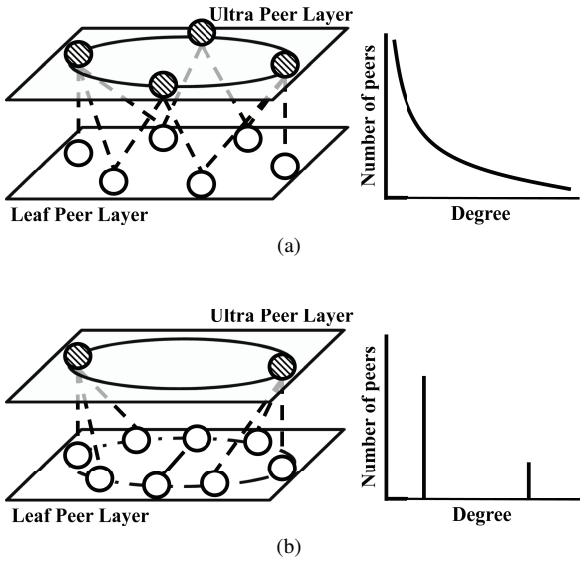


Fig. 1. Comparison of hierarchical unstructured P2P models and their degree distributions. (a) The modern Gnutella networks. (b) The proposed networks (THUP).

On the other hand, the network characteristics of Gnutella have been analyzed and measured in many works [5]–[8]. According to these works, the Gnutella network has a power-law degree distribution as depicted in Fig. 1(a), where almost all of the real-world networks such as Internet, Word Wide Web (WWW) [9], and some social networks have the same degree distribution. While power-law degree distribution can be tolerant to churn, i.e., the dynamics of peer participation and departure (or fault), it cannot be tolerant to Denial of Service (DoS) attacks [10], i.e., the highest degree peers are preferentially removed. In other words, a malicious attacker may easily disrupt the Gnutella network since the removal of the highest degree peers would have a significant impact on the entire network. In fact, the research work in [8] shows that the removal of high degree peers causes the disruption of Gnutella networks, and this is evident following the removal of only 4% of the peers. Therefore, in order to construct hierarchical unstructured P2P networks tolerant to DoS attack, appropriate topologies have to be designed and used.

The main objective of this paper is improving the stability of hierarchical unstructured P2P networks against churn and DoS. Similar to the modern Gnutella network consisting of two types of peers, we envision a novel P2P network, based on bimodal degree distribution, as shown in Fig. 1(b). This

implies that our envisioned P2P network also comprises two types of peers [11], [12]. Compared with power-law degree distribution, bimodal degree distribution can be tolerant to both churn and DoS attacks. Furthermore, since the stability of the proposed P2P network is affected by its neighbors selection, we present an optimal topology in terms of the impact of the DoS attacks. Our proposed scheme, dubbed THUP (churn and Dos Tolerant, Hierarchical, Unstructured, P2P network), employs the proposed topology based on bimodal degree distribution. In addition, we propose a peer joining procedure in the proposed scheme.

The remainder of this paper is organized as follows. A summary of the relevant research work on the P2P networks tolerant to both churn and DoS attacks is presented in Section II. In Section III, we analyze churn and DoS attacks in hierarchical unstructured P2P networks in order to measure the stability of the considered networks. We present our envisioned P2P architecture, dubbed THUP, in Section IV along with a novel peer joining procedure. Section V evaluates the performance of THUP in terms of both network connectivity and communication efficiency through extensive computer simulations. Finally, concluding remarks are provided in Section VI.

II. Related Work

Since peers can freely join and depart in unstructured P2P networks, isolation of peers may be caused [13]. In order to overcome this shortcoming, the stability of unstructured P2P networks against peer departures is critical for ensuring efficient performance as addressed in numerous works [14]–[17]. These works conducted in [3], [4] approach peer departures tolerance by using the super peer. Although these research works achieve high performance and reduced management overheads such as neighbor selection and link maintenance and so on, the proposed networks are intolerant to super peer targeted attacks, just like modern Gnutella network, which consist of ultra peer and leaf peer. In [18]–[20], in oder to prevent the network disruption with peer departures, the authors present two age-independent neighbor selection schemes. However, these schemes assume exponential session lengths and may not actually be able to improve the stability of the networks. The session lengths in actual unstructured P2P networks are not exponential as shown by the work in [13]. Other efforts focus on random networks following binomial degree distribution that ensure the stability against peer departures [21], [22]. In order to construct random networks, each peer requires global knowledge, which includes the number of peers in the whole network, the degree of each peer, and so forth. So, these works adopt gossip-based membership management protocols for global knowledge.

On the other hand, designing unstructured P2P networks tolerant to attacks is also important, since performance of the networks substantially diminish by the attacks, which include specific and non-specific attacks in P2P networks [23]. Especially targeted attacks such as DoS can cause disruption of the P2P networks; therefore, the work should conduct improving stability of the networks against targeted attacks. However, there has been little research work in literature concerning the targeted attacks in unstructured P2P networks. The research work conducted in [12] analyzes the degree distribution of super-peer P2P networks to figure out the stability against both targeted attacks and peer departures. Unfortunately, the critical issue of enhancing the network stability is not stressed upon in this work. In [24], a method to enhance the stability of P2P networks based on spanning trees is proposed. While this work presents an analytical model to assess the stability and describe the attack strategies, it is rather limited to live multimedia streaming applications.

In this paper, one of our contributions consists in opening up a new direction in hierarchical unstructured P2P networks, namely the optimal degree distribution and neighbor selection method against both departures and targeted attacks. In other words, our work brings up the yet to be studied important issue of network stability under node departure events and DoS attacks, which would break down modern P2P networks including the popular Gnutella.

III. Churn and DoS models

In this section, we propose analytical models to evaluate the stability of P2P networks under the effect of churn and DoS attacks. Churn and DoS attacks in a P2P network may be modeled in terms of removing peers from the considered network by taking into account that the probability of removing each peer is determined by the number of links connected to the peer (i.e., by the degree of the peer).

The churn refers to the effect of independent participation and departure by thousands of peers. Churn degrades the performance and the stability of the network since the peers become isolated due to departure of their neighboring peers. Thus, the peer departures in hierarchical unstructured P2P networks are modeled in order to evaluate the stability of networks against churn. In the case of the peer departures separating the peer from the network due to mechanical troubles, user operation, and so on, a peer is removed randomly regardless of the degree of the peer. Here, $K = \{k_1, k_2, ..., k_m\}$ is the set that the degree of peers is arranged in an ascending order, where m denotes the mode number of the set. Let q be the probability that a peer is removed randomly and b_k be the probability that a peer of degree k survives after removing the peers. $p = \sum_k b_k P(k)$ indicates the fraction of peers that have survived after removing the peers. Here, $P(k)$ denotes the degree distribution of peers before removing the peers. Hence, the peers departure model b_k^{churn} is defined by the following equation.

$$b_k^{\text{churn}} = p \equiv 1 - q, \quad k \in K. \tag{1}$$

In case of the DoS attacks, the probability of removal of each peer is supposed to be proportional to the degree of the peers since malicious attackers may disrupt the performance of the networks. In hierarchical unstructured P2P networks, which consist of two type of peers, i.e., ultra peers and leaf peers, malicious attackers may target only ultra peers since the removal of the peers substantially influence network connectivity. Therefore, we consider the DoS model in ultra

peers and leaf peer in a separate fashion. Let $P_{\rm ultra}(k)$ and $P_{\rm leaf}(k)$ be the degree distribution of ultra peers and leaf peers, respectively. $K_{\rm ultra} = \{k_u, k_{u+1}, ..., k_m\}$ and $K_{\rm leaf} = \{k_1, k_2, ..., k_l\}$ are sets of the degree of ultra peers and leaf peers, respectively, where $k_u \gg k_l$, k_u and k_l refer to the minimal degree of ultra peers and the maximal degree of leaf peers, respectively. Since malicious attackers target the highest degree of ultra peers in a DoS attack, the removal method of ultra peers in the hierarchical unstructured P2P networks $ub_k^{\rm DoS}$ can be formulated as follows.

$$ub_k^{\rm DoS} = \begin{cases} 1, & \text{if} \quad \{k \in K_{\rm ultra} | k < k_{m'}\}, \\ ub_{k_{m'}}^{\rm DoS}, & \text{if} \quad \{k \in K_{\rm ultra} | k = k_{m'}\}, \\ 0, & \text{if} \quad \{k \in K_{\rm ultra} | k > k_{m'}\}, \end{cases} \tag{2}$$

where, m' denotes the maximal mode number of the set $K_{\rm ultra}$ after removal of peers. Leaf peers may depart from networks randomly even while suffering a DoS attack in the network. Thus, leaf peers are removed randomly regardless of the degree of the peer. Hence, the removal method of leaf peers in hierarchical unstructured P2P $lb_k^{\rm DoS}$ networks can be expressed as follows.

$$lb_k^{\rm DoS} = p \equiv 1 - q, \quad k \in K_{\rm leaf}. \tag{3}$$

Thus, we propose the DoS model in hierarchical unstructured P2P which is a combination of $ub_k^{\rm DoS}$ and $lb_k^{\rm DoS}$, namely ultra peers are firstly removed according to Eq. (2), and then leaf peers are removed according to Eq. (3).

IV. Hierarchical Unstructured P2P Networks Tolerant to Churn and DoS attacks

In hierarchical unstructured P2P networks such as modern Gnutella and Kazaa, the tolerance to departures and the communication efficiency are high because there are ultra peers (or super peers) which increase the network connectivity [25]. However, the ultra peers may confront a threat from attacks that the highest degree peer is targeted because their removal has an enormous amount of adverse influence over the networks. There are three conditions to achieve high stability of targeted attacks, namely (i) increasing the average degree of peers, (ii) conducting the most suitable degree distribution, and (iii) a topology tolerant or resilient to adverse effects of the attack. The first condition cannot be satisfied in large-scale P2P networks due to the enormous amount of network operating overhead and link maintenance cost. As for the second condition, a uniform distribution with all peers having a constant degree demonstrates the highest performance [26]. However, the communication efficiency, which is absolutely imperative to construct large-scale P2P networks, is extremely low in the uniform distribution due to non-existence of peers having higher degrees than other peers. Therefore, in order to achieve high robustness against churn and DoS, and to increase the communication efficiency, we apply a bimodal degree distribution based on the concept introduced by T. Tanizawa *et al* [11]. Further details about bimodal degree distribution are provided in Section IV-A. To the best of our knowledge, the topology construction method based on bimodal degree distribution has not been proposed in previous studies. This paper is considered as a first approach that conducts optimal topology for tolerance of both churn and DoS attacks. Designing an appropriate topology is of significant importance to construct tolerant networks. For example, if all of the neighbors of a given peer are formed by ultra peers, the peer is vulnerable against targeted attacks since ultra peers are preferentially attacked. In Section IV-B, we present an optimal topology (which we refer to as THUP throughout the paper) for hierarchical unstructured P2P networks tolerant to DoS attacks. On the other hand, the topology in P2P networks dynamically change due to peers participation and departure events. It is, therefore, difficult to continue using the same optimal topology. As a consequence, in Section IV-C, we propose a peer joining procedure to approximate the optimal topology even under changing network dynamics.

A. Bimodal Network

According to the work of T. Tanizawa *et al* [11], we expect that exploiting bimodal degree distribution may lead to high stability of networks against both departures and targeted attacks, resulting in improved communication efficiency. The features of bimodal degree distribution are presented in the following. There are only two different categories of peers, namely peers having a constant high degree $k_{\rm ultra}$, and those with a constant low degree $k_{\rm leaf}$. Each degree of $k_{\rm ultra}$ and $k_{\rm leaf}$, which optimizes performance in tolerance of departures and targeted attack, is given by the following function.

$$k_{\rm ultra} = \sqrt{\langle k \rangle N}, \tag{4}$$

$$k_{\rm leaf} = \langle k \rangle, \tag{5}$$

where $\langle k \rangle$ is the average degree of the network. The number of peers, N, can be represented as follows.

$$N = N_{\rm ultra} + N_{\rm leaf} = rN + (1 - r)N, \tag{6}$$

where $N_{\rm ultra}$ and $N_{\rm leaf}$ are the number of ultra peers and that of leaf peers, respectively. The ratio of the number of ultra peers to the number of all the peers, denoted by r, also optimizes stability of the networks. Note that r is derived from statical analysis as follows.

$$r = \left(\frac{A^2}{\langle k \rangle N} \right)^{\frac{3}{4}}, \tag{7}$$

$$A = \left\{ \frac{2\langle k \rangle^2 (\langle k \rangle - 1)^2}{2\langle k \rangle - 1} \right\}^{\frac{1}{3}}. \tag{8}$$

Thus, the bimodal degree distribution can be expressed by N and $\langle k \rangle$ as follows:

$$P(k) = \begin{cases} (1 - r)N, & \text{if} \quad k = \langle k \rangle, \\ rN, & \text{if} \quad k = \sqrt{\langle k \rangle N}, \\ 0, & \text{otherwise.} \end{cases} \tag{9}$$

Bimodal degree distribution has mixed features from both uniform and power-law degree distributions as identified above, inheriting targeted attacks tolerance from uniform degree distribution and departures tolerance from power-law degree distribution. In contrast with the power-law degree distribution,

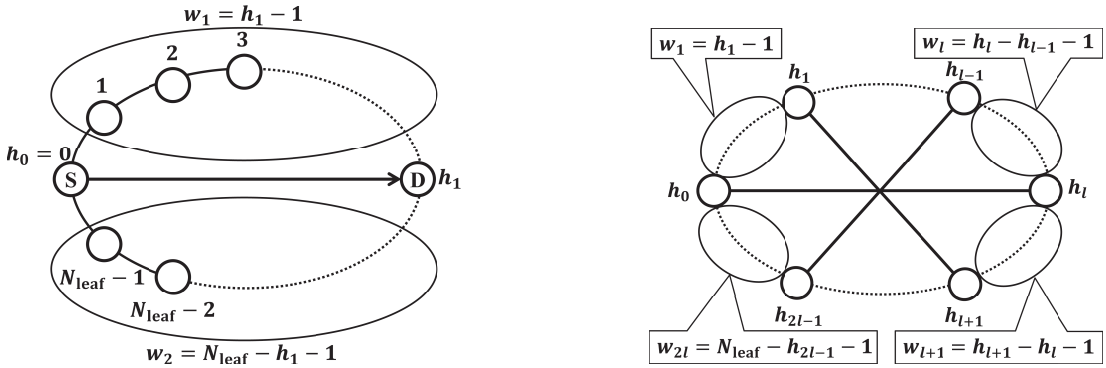


Fig. 2. The location of source and destination extra peers (a) network having 1 extra link. (b) network having l extra links.

the bimodal degree distribution can achieve high tolerance of targeted attacks since the existence of only two types of peer reduces the vulnerability against targeted attacks [26]. On the other hand, the existence of high degree peers increases the performance of departures tolerance and communication efficiency compared with uniform degree distribution [11].

B. Optimal topology for DoS tolerance

The links can be classified into three categories in the network based on bimodal degree distribution, namely, the links in the ultra peer layer, in the leaf peer layer, and between the ultra and the leaf peer layers. In the ultra peer layer, each ultra peer connects with the other ultra peers since there exist a lot of traffic in the ultra peer layer. Therefore, the number of the links in the ultra peer layer, l_{ultra}, is decided as $N_{\text{ultra}}(N_{\text{ultra}}-1)/2$. Thus, the number of the links between layers $l_{\text{interlayer}}$ becomes equal to $N_{\text{ultra}}\{k_{\text{ultra}}-(N_{\text{ultra}}-1)\}$, and, the number of the links in the leaf peer layer l_{leaf} is decided as $(N_{\text{leaf}}k_{\text{leaf}} - l_{\text{interlayer}})/2$. Here, we define that each leaf peer has one link between the layers. On the other hand, the neighbor selection in ultra peer layer and between the layers do not influence the tolerance to DoS attack since ultra peers are firstly removed as modeled by Eq. (2). Thus, we address the topology in the leaf peer layer.

Leaf peer layer basically employs a ring topology. The topology ensures that leaf peers are equally privileged, i.e., they have equal degrees. For example, if $k_{\text{leaf}} = 2$, the topology, in which leaf peers have equal degrees, is limited to only ring topology. The number of links for constructing a ring topology l_{ring} becomes equal to the number of the leaf peers, N_{leaf}. And therefore, some peers have the links not involving for a constructing a ring topology called extra link if $l_{\text{leaf}} > l_{\text{ring}}$. Peers having extra link are called extra peers. Here, assuming that each extra peer has an extra link, the number of extra peers becomes equal to the number of extra links. The number of extra links, denoted by l_{extra}, is decided as follows:

$$l_{\text{extra}} = l_{\text{leaf}} - l_{\text{ring}}. \tag{10}$$

Since the extra links influence the stability of the networks, we focus on the location of the extra peers.

First, we are interested in the optimal location of the source and destination peers in the network having 1 extra link, i.e. the network consists of a ring topology and an extra link. Fig. 2(a) is an example where the destination peer is the h_1 neighboring peer in clockwise direction from the source peer with $2 \leq h_1 \leq (N_{\text{leaf}}/2)$. The ring topology can be regarded as divided by extra peers into two segments, w_1 and w_2. They are defined as (h_1-1) and $(N_{\text{leaf}}-h_1-1)$, respectively. Here, we quantify the network disruption probability. Since the network can be disrupted by removing only two peers, we consider the scenario where two peers are removed in a random manner. The network disruption events can be classified into two types, namely the network disruption by the removal of any of the peers after the removal of one of extra peers, and by the removal of any of the peers after the removal of a non-extra peer. Thus, the network disruption probability can be formulated as follows.

$$\begin{aligned} P(h_1) &= \frac{2(N_{\text{leaf}}-3)}{N_{\text{leaf}}(N_{\text{leaf}}-1)} \\ &\quad + \frac{1}{N_{\text{leaf}}(N_{\text{leaf}}-1)}\{(h_1-1)(h_1-1)-1) \\ &\quad + (N_{\text{leaf}}-h_1-1)(N_{\text{leaf}}-h_1-1)-1)\}. \\ &= \frac{2h_1(h_1-N_{\text{leaf}}) + (N_{\text{leaf}}-2)(N_{\text{leaf}}+1)}{N_{\text{leaf}}(N_{\text{leaf}}-1)}. \end{aligned} \tag{11}$$

Since it is clear from the above equation that the network disruption probability is a quadratic function of h_1, the optimal value of h, which minimizes the network disruption probability can be decided as follows.

$$h_1^{opt} = \arg\min_{h_1} P(h_1) = \frac{N_{\text{leaf}}}{2}. \tag{12}$$

It can be concluded that the source extra peer should select $(N_{\text{leaf}}/2)$-hops away peers as destination extra peers.

The above analysis can be easily applied to the networks with multiple extra links as depicted in Fig. 2(b) where non-extra peers are divided into $g = 2l$ segments by l extra links. The probability of network disruption with the removal of two peers can be formulated in the similar way as before by using

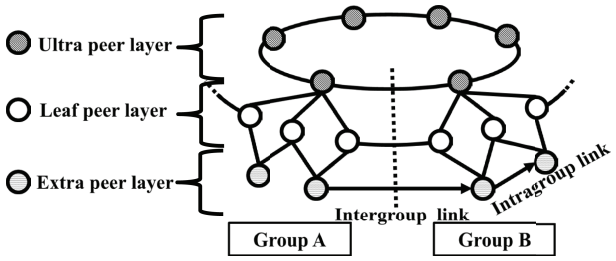


Fig. 3. The general idea that the network is split into a number of groups in order to approximate the proposed topology.

the size of each segment as below.

$$\begin{aligned} P(h_l) &= \frac{\sum_{i=1}^{g-1}(w_i + w_{i+1}) + w_1 + w_g}{N_{\mathrm{leaf}}(N_{\mathrm{leaf}} - 1)} \\ &\quad + \frac{\sum_{i=1}^{g} w_{\mathrm{i}}(w_{\mathrm{i}} - 1)}{N_{\mathrm{leaf}}(N_{\mathrm{leaf}} - 1)} \\ &= \frac{(N_{\mathrm{leaf}} - g) + \sum_{i=1}^{g} w_i^2}{N_{\mathrm{leaf}}(N_{\mathrm{leaf}} - 1)}. \end{aligned} \tag{13}$$

Since there is a condition that the summation of w_i is a constant value equal to $(N_{leaf} - g)$, we can conclude that the network disruption probability takes its minimum value when the segment size is equal in all segments, i.e., $w_i = N_{leaf}/g - 1$.

C. Peer joining procedure in THUP

We have presented optimal hierarchical topology for tolerant to both churn and DoS attacks based on bimodal degree distribution, called THUP. However, the realization of THUP is, indeed, complex, since the hop count in P2P networks dynamically changes with peers departure and participation events. To deal with this issue, we propose a solution whereby the considered P2P network is split into several groups, which consist one ultra peer and a number of leaf peers, as demonstrated in Fig. 3. The link between two peers in different groups and that in the same group are called inter-group link and intra-group link, respectively. The selection of peers from different groups as neighbors (i.e., from inter-group peers) enhances the probability that the segment size is equal in all segments than that from the intra-group peers. Therefore, the number of inter-group links becomes equal to the number of the extra links defined by Eq. (10). In this subsection, we propose a peer joining procedure in THUP as shown in Alg. 1.

First, a newly joining peer receives the following inter-group list from the ultra peers: the number of peers in the whole network, and the details of each group (i.e., the ultra peer's address, the number of peers in each group, and the number of candidates, one of which is used to construct an inter-group link). Second, the newly joining peer determines its type, which is calculated according to the difference between the current and the ideal degree distributions. The current value of the number of ultra peers N'_{ultra} and leaf peers N'_{leaf} can be obtained from the global knowledge of the system. On the other hand, the ideal numbers of each peer layer N_{ultra} and N_{leaf} are calculated by using Eq. (7) with the average degree

Algorithm 1 Peer joining algorithm in THUP.

```
Get inter-group list
if ε_leaf ≤ ε_ultra then
  Affiliate with ultra peer
  The degree is k_ultra
  Get inter-group list
  Connection with other ultra peers
else
  Affiliate with leaf peer
  Decide on one's own group
  The degree is k_leaf
  Get intra-group list
  if The degree of ultra peer is not fully filled then
    Connection with ultra peer
  end if
  Insertion process
  while One's own degree is not fully filled do
    Expansion process
    if Have sufficient degree then
      Break
    end if
    if No candidate for neighbor then
      Break
    end if
  end while
end if
Register self-information to the intra-group list.
```

$\langle k \rangle$ and the number of peers N. Thus, the difference between the current and ideal number in the ultra peers and that in the leaf peers are decided as follows.

$$\varepsilon_{\mathrm{ultra}} = \|N_{\mathrm{ultra}} - N'_{\mathrm{ultra}}\|, \tag{14}$$

$$\varepsilon_{\mathrm{leaf}} = \|N_{\mathrm{leaf}} - N'_{\mathrm{leaf}}\|. \tag{15}$$

When ($\varepsilon_{\mathrm{ultra}} > \varepsilon_{\mathrm{leaf}}$), the type of a newly joining peer is decided to be an ultra peer, otherwise it is considered to be a leaf peer.

In the case of the ultra peer, the newly joining ultra peer communicates with other ultra peers for obtaining the inter-group list. The degree of the ultra peer is calculated according to Eq. (4) by using the number of peers including the newly joining peer (it is worth noting that degree of the ultra peer changes in a dynamic fashion). Then, the ultra peer connects with other ultra peers.

The action in the case of leaf peers is described in the following. Initially, the newly joining leaf peer attempts to decide on the affiliation group with the help of ultra peers using the inter-group list, namely the group having the minimum number of peers is selected as the affiliation group. Then, it receives the intra-group list from the ultra peer in affiliation group that contains the average degree, the degree of ultra peer, the number of peers in the whole network, and the details of each peer in the group (i.e., the peer's address including both ultra and leaf peers, and peer type such as ultra or leaf peer). The degree of the newly joining leaf peer is decided using the inter-group list. The leaf peer attempts to connect with the ultra

peer if the degree of the ultra peer is not fully filled. Moreover, The leaf peer follows two consecutive connection procedures. In order to set up the links to optimally select neighbors, the procedures consist of two steps, namely (i) insertion phase, and (ii) expansion phase, which are described as follows.

(i) *Insertion Phase* – The objective of the insertion phase is to construct a ring topology in leaf peer layer to provide all the peers with an equal opportunity to establish connections.

In the insertion phase, the newly joining peer randomly selects a link in one's own group, and inserts itself into the link. In this vein, it breaks the existing link and creates new links between itself and each peer.

(ii) *Expansion Phase* – Following the insertion phase, the leaf peer moves to the expansion phase, in which the peer establishes links as long as the degree of the peer is lower than the average degree $\langle k \rangle$ or the candidate for the neighbor peers is in the inter-group list. Here, the candidate peers are leaf peers, which have a lower degree than the average degree $\langle k \rangle$. In order to make inter-group links, the leaf peer needs to find the candidate in other groups. Therefore, the ultra peer in one's own group searches the candidate by using the inter-group list. The leaf peer connects with the candidate after being found by its ultra peer. This also prompts the ultra peer to accordingly update the inter-group list. Since the degree of the peers is limited by the average degree and the candidates become insufficient, it is possible that the newly joining peer cannot make an adequate number of links. In such a situation, the peer temporarily waits for the participation of other peers until the condition is satisfied. Thus, the newly joining peers (regardless the type of peers) adds self-information to the intra-group list, which is shared in each group.

V. Performance Evaluation

In this section, we evaluate the performance of the proposed THUP selection scheme through extensive computer simulations by using Ruby [27]. The performance evaluation is composed of two parts. In the first part, we verify the performance of neighbor selection in THUP, i.e., we investigate the impact of the number of inter-group links on the clustering coefficient and tolerance of both DoS attacks and churn. Then, we evaluate the performance of THUP, compared with other hierarchical unstructured P2P networks, namely modern Gnutella [5]–[8], and bimodal network which is constructed by the random neighbor selection based bimodal degree distribution. In order to quantify the performance of THUP, three different metrics [28], [29], namely (i) global network connectivity, (ii) local network connectivity, and (iii) communication efficiency, are used.

In all the conducted simulations, the average degree of each network is set to 3, and two different types of network failures, due to DoS attacks and Churn, are simulated to consider the removal of peers from the network. The model of DoS attack (as represented by Eqs. (2) and (3)) remove the highest degree peers from the ultra peers layer and random ones from the leaf peers level. On the other hand, peers are randomly simulated to leave the considered network following the churn model, as represented by Eq. (1).

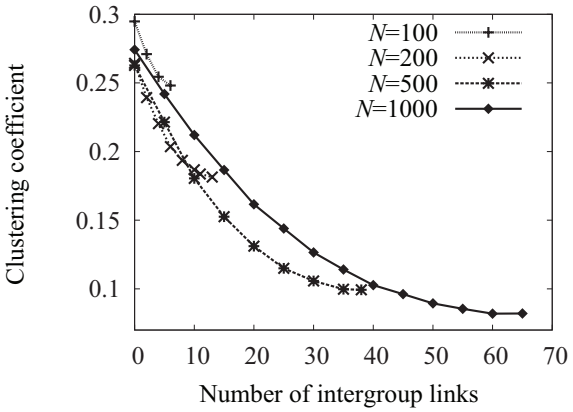


Fig. 4. Relation between number of inter-group links and clustering coefficient.

A. Verifying the performance of THUP

In order to achieve tolerance to DoS attacks, the leaf peers are structured in a ring topology, and some of them are simulated to have an extra link. In our scheme, the DoS tolerance is enhanced by conforming with the segments size $N_{\text{leaf}}/g - 1$. At least, the segment size must not become one. In other words, the source extra peer must not select any 2-hop away peer as its destination. Here, establishing a link between 2-hop neighbor peers is referred to as a clustering event. Thus, in order to evaluate the tolerance of networks, we compute the average clustering coefficient, C in the network, given by the following equation [30].

$$C = \frac{1}{N}\sum_{i} C_i, \tag{16}$$

$$C_i = \frac{2M_i}{k_i(k_i-1)}, \tag{17}$$

where C_i, k_i, and M_i denote the cluster coefficient, the degree, and the number of links between the neighbor peers of the i^{th} peer, respectively. The lower value of C implies that there exist a few clusters in the network and the network achieves high tolerance to DoS attacks.

On the other hand, in our scheme, the extra link is classified into the inter-group link and the intra-group link. Since establishing an inter-group link decreases the probability of the existence of clusters than creating an intra-group link, increasing the number of inter-group links enhances the resiliency against DoS attacks. Fig. 4 demonstrates the average clustering coefficient, C, with different numbers of inter-group links l_{inter} in different numbers of peers. The number of peers is set to any of the following values $\{100, 200, 500, 1000\}$. It is obvious that the average clustering coefficient is decreased by increase of the number of inter-group links. Thus, THUP can minimize the number of clusters in the network by setting the number of inter-group links to the number of extra links.

Next, we investigate the impact of the number of inter-group links on the global network connectivity of both DoS attacks and churn in THUP as demonstrated in Fig. 5. We can evaluate the global network connectivity through the introduction on critical threshold, f, which quantifies how many peers can be left from a network without disrupting the network, given by

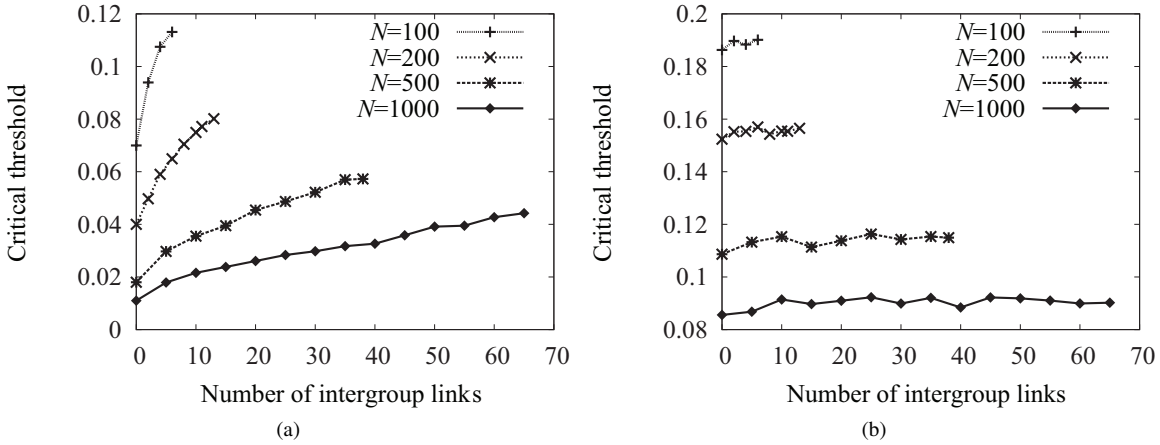


Fig. 5. Impact of the number of inter-group links on the critical threshold in the proposed network. (a) in case of DoS; (b) in case of of churn.

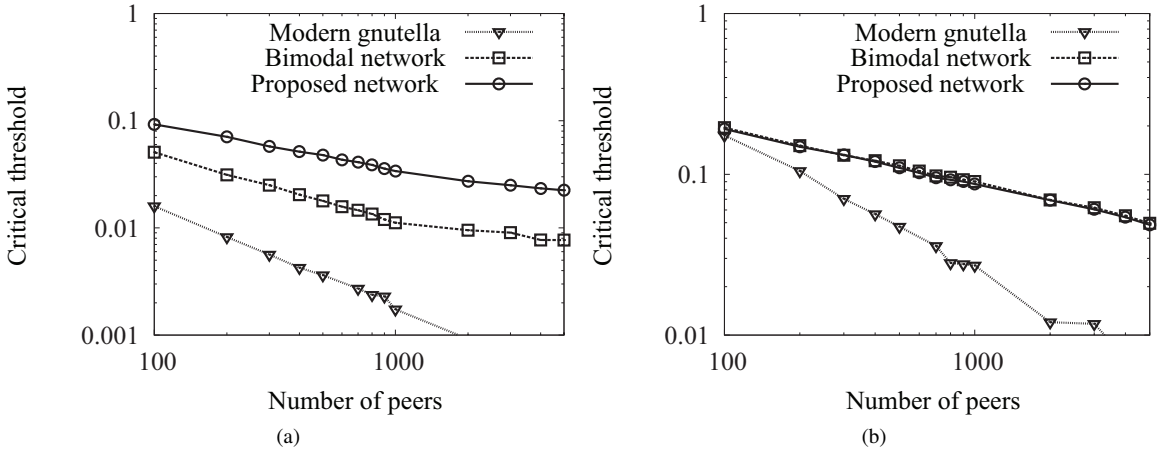


Fig. 6. Tolerance of global network connectivity in different sizes and types of networks. (a) in case of a DoS attack; (b) in case of churn.

the following equation.

$$f = \frac{N_{\rm th}}{N}, \quad (0 \leq f \leq 1), \tag{18}$$

where N denotes the number of peers in the whole network, and $N_{\rm th}$ denotes the number of peers, which can be removed from the network without the network disruption. Note that f closer to 1 is necessary to achieve a high level of global network connectivity. While the tolerance of churn is kept regardless the number of inter-group links, the tolerance of DoS attacks can be improved by increasing the number of inter-group links. Thus, the result from these simulations indicates that, the tolerance of DoS attacks can be enhanced by minimizing the average clustering coefficient in THUP by setting the number of inter-group links to the number of extra links.

B. Performance comparison in global network connectivity.

We evaluate the global connectivity of networks by using critical threshold, f. Fig. 6 demonstrates the critical threshold in case of a DoS attack and churn with different number of peers in each network, namely, modern Gnutella, network based bimodal degree distribution without the proposed neighbor selection called bimodal network, and THUP, respectively. The number of peers is varied from 100 to 5000. In case of the DoS attack, THUP exhibits the highest tolerance than other networks. In particular, compared with the modern Gnutella network, the performance of THUP is significantly high despite the fact that both of these schemes employ hierarchical structures. In addition, the result of comparison between the THUP and bimodal network clearly demonstrates that the proposed neighbor selection method is the most effective one. In case of churn, THUP and the bimodal network have a higher tolerance compared with the modern Gnutella network. Considering both DoS and churn, it is evident that THUP is, indeed, the most suitable network.

C. Performance comparison in local network connectivity

We refer to the local network connectivity, which is a number of networks structured by remaining peers, following the network disruption. If the network splits into a number of smaller networks, each peer is unable to do find its desired target resource (e.g., file that it wants to download). However, if the network splits into two micro and macro networks, almost all of the peers remain unaffected. Therefore, we

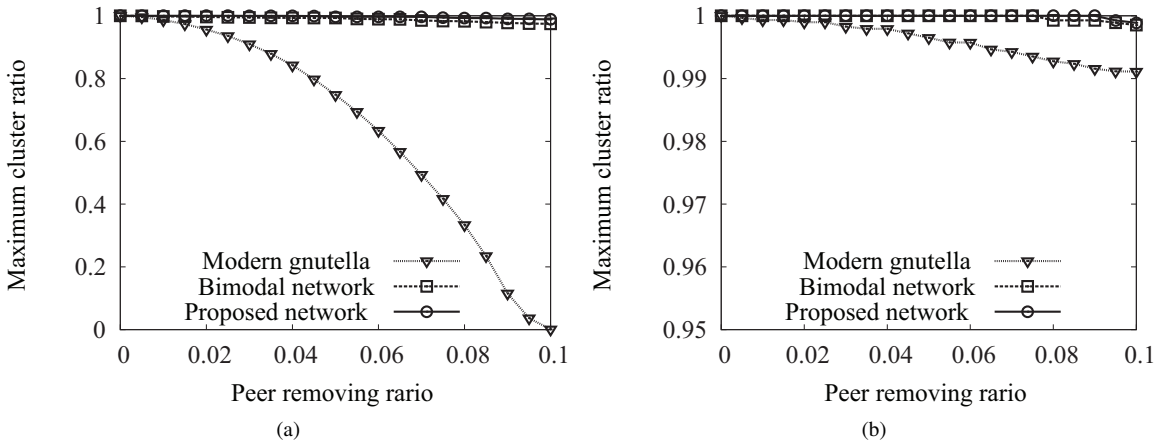


Fig. 7. Impact of peer removing ratio on tolerance of local network connectivity in different types of networks. (a) in case of a DoS attack; (b) in case of churn.

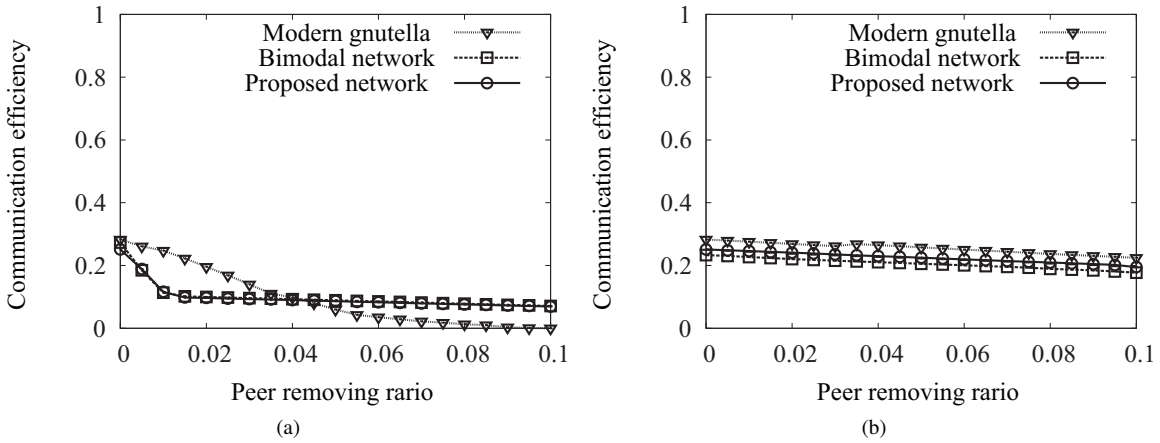


Fig. 8. Impact of peer removing ratio on communication efficiency in different types of networks. (a) in case of a DoS attack; (b) in case of churn.

evaluate the tolerance of local network connectivity using the maximum cluster ratio S, which denotes the ratio of the size of the maximum cluster to that of the original network. This explains the reason that the maximum cluster ratio signifies the impact of the network disruption on the number of utilized peers. It is defined as follows.

$$S = \frac{N_{\mathrm{mc}}}{N_{\mathrm{rmv}}}, \quad (0 \leq S \leq 1), \tag{19}$$

where N_{mc} denotes the number of peers in the maximum cluster, and N_{rmv} represents the number of peers after the removal peers. S closer to 1 implies a higher local network connectivity, which also means that a number of peers remain free from the influence of network disruption.

Fig. 7 depicts the impact of peer removing ratio, r, on the tolerance of local network connectivity in each network. To evaluate the tolerance in terms of realistic probabilities of DoS and churn, the value of r is varied in the range from zero to 10^{-1}, and the number of peers is set to 10^3. In case of DoS, while the modern Gnutella network falls to an extremely low tolerance with a progressive increase of peer removing ratio, other networks achieve relatively high performance, which closes on the best value. In case of churn, the value of S in the modern Gnutella network is also lower than the others. These results indicate that THUP is able to inhibit peer isolation, namely peers are able to find their intended file in THUP more effectively than the existing methods.

D. Performance comparison in communication efficiency

We can conclude that THUP is the best choice on the issue of DoS and churn tolerant P2P network since it achieves the highest tolerance in contrast with the other networks. From hereon, we study on unstructured P2P networks has been conducted from the points of view of communication efficiency, and demonstrate that THUP is as competent as the modern Gnutella network. The communication efficiency is defined by the following equation.

$$E = \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{ij}}, \quad (0 \leq E \leq 1), \tag{20}$$

where d_{ij} is the number of hops between the i^{th} and j^{th} peers. Here, if there is no available path between two peers, the hop count between them is infinity large, i.e., the inverse of the hop count is equal to zero. Therefore, network failures degrade the communication efficiency. The maximum value of E is one,

which implies a complete graph, and a larger value indicates higher communication efficiency. Moreover, the value of E of the applicable P2P networks must be higher than 0.1 [2].

Fig. 8 demonstrates the values of E for different value of the removing ratio, r, in each network. This simulation is conducted with the same setting as in the evaluation of the local network connectivity. In both the cases of DoS attacks and churn, the communication efficiency of THUP is nearly equal to that of the modern Gnutella. Moreover, the value of E of modern Gnutella is lower than 0.1 after removing only 4% of the peers in case of the DoS attacks. Therefore, modern Gnutella is not well suited for DoS attacks. It is demonstrated that THUP can offer not only high connectivity resulting in high tolerance of DoS and churn but also high communication efficiency. Thus, we conclude that the proposed THUP features as the most suitable network in this research area.

VI. Conclusion

One of the key study areas of unstructured P2P networks is to achieve high tolerance of DoS attacks and churn. Despite their popularity, unstructured P2P networks such as Gnutella and Kazaa are vulnerable to the threat of DoS attacks. We address this issue in this work that was not covered in existing studies. Our approach is focused on the degree distribution of P2P networks. Since the modern Gnutella follow the power-law degree distribution, it is intolerant to a higher peer targeted attacks such as DoS. Therefore, we introduce bimodal degree distribution to the unstructured P2P network. In addition, we conduct an optimal topology for DoS tolerance, dubbed THUP. In order to construct the optimal topology, we also propose a peer joining procedure based on grouping. We verify the effectiveness of THUP through extensive computer simulations. In particular, we demonstrated that the P2P network can offer high network connectivity, which increases the tolerance of DoS attacks and churn, thereby ensuring significantly higher communication efficiency in contrast with the modern Gnutella network. We expect that the proposed THUP may be widely applied to file sharing systems, multimedia streaming, and so forth.

References

[1] S. Saroiu, K. P. Gummadi, and S. D. Gribble, "Measuring and analyzing the characteristics of napster and gnutella hosts," *Multimedia Systems*, vol. 9, no. 2, pp. 170–184, Aug. 2003.

[2] E. K. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, "A survey and comparison of peer-to-peer overlay network schemes," *IEEE Communications Surveys and Tutorials*, vol. 7, no. 2, pp. 72–93, 2005.

[3] J. Lin and M. Yang, "Robust super-peer-based p2p file-sharing systems," *Computer journal*, vol. 53, no. 7, pp. 951–968, Sep. 2010.

[4] L. Garcs-Erice, E. W. Biersack, K. W. Ross, P. A. Felber, and G. Urvoy-Keller, "Hierarchical peer-to-peer systems," *Parallel Processing Letters*, vol. 13, no. 4, pp. 643–657, Dec. 2003.

[5] M. Ripeanu, A. Iamnitchi, and I. Foster, "Mapping the gnutella network," *IEEE Internet Computing*, vol. 6, no. 1, pp. 50–57, Jan.-Feb. 2002.

[6] Y. Wang, X. Yun, and Y. Li, "Analyzing the characteristics of gnutella overlays," in *Proc. of International Conference on Information Technology-New Generations*, Las Vegas, Nevada, USA, Apr. 2007, pp. 1095–1100.

[7] D. Stutzbach, S. Zhao, and R. Rejaie, "Characterizing files in the modern gnutella network," *Multimedia Systems*, vol. 13, no. 1, pp. 35–50, Mar. 2007.

[8] D. Stutzbach, R. Rejaie, and S. Sen, "Characterizing unstructured overlay topologies in modern p2p file-sharing systems," *IEEE/ACM Transactions on Networking*, vol. 16, no. 2, pp. 267–280, Apr. 2008.

[9] R. Albert, H. Jeong, and A.-L. Barabasi, "Error and attack tolerance of complex networks," *Nature*, vol. 401, pp. 130–131, Sep. 1999.

[10] Y. Jiang, C. Lin, M. Shi, X. S. Shen, and X. Chu, "A dos and fault-tolerant authentication protocol for group communications in ad hoc networks," *Computer Communications*, vol. 30, no. 11-12, pp. 2428–2441, Sep. 2007.

[11] T. Tanizawa, G. Paul, R. Cohen, S. Havlin, and H. E. Stanley, "Optimization of network robustness to waves of targeted and random attacks," *Physical Review E*, vol. 71, no. 4, Apr. 2005.

[12] B. Mitra, F. Peruani, S. Ghose, and N. Ganguly, "Analyzing the vulnerability of superpeer networks against attack," in *Proc. of the 14th ACM conference on Computer and communications security*, Alexandria, Virginia, USA, Oct.-Nov. 2007, pp. 225–234.

[13] D. Stutzbach and R. Rejaie, "Understanding churn in peer-to-peer networks," in *Proc. of the ACM SIGCOMM*, Pisa, Italy, Sep. 2006, pp. 189–202.

[14] Y. Chawathe, S. Ratnasamy, L. Breslau, N. Lanham, and S. Shenker, "Making gnutella-like p2p systems scalable," in *Proc. of SiGCOMM 2003*, vol. 33, Karlsruhe, Germany, Aug. 2003, pp. 407–418.

[15] G. Pandurangan, P. Raghavan, and E. Upfal, "Building low-diameter peer-to-peer networks," *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 6, pp. 995–1002, Aug. 2003.

[16] V. Vishnumurthy and P. Francis, "On heterogeneous overlay construction and random node selection in unstructured p2p networks," in *Proc. of IEEE INFOCOM*, Barcelona, Spain, Apr. 2006.

[17] C. Vassilakis and I. Stavrakakis, "Minimizing node churn in peer-to-peer streaming," *Computer Communications*, vol. 33, no. 14, pp. 1598–1614, Sep. 2010.

[18] D. Leonard, Z. Yao, V. Rai, and D. Loguinov, "On lifetime-based node failure and stochastic resilience of decentralized peer-to-peer networks," *IEEE/ACM Transactions on Networking*, vol. 15, no. 3, pp. 644–656, Jun. 2007.

[19] Z. Yao, X. Wang, D. Leonard, and D. Loguinov, "Node isolation model and age-based neighbor selection in unstructured p2p networks," *IEEE/ACM Transactions on Networking*, vol. 17, no. 1, pp. 144–157, Feb. 2009.

[20] H. Liu, X. Liu, W. Song, and W. Wen, "An age-based membership protocol against strong churn in unstructured p2p networks," in *Proc. of International Conference on Network Computing and Information Security*, vol. 2, Guilin, China, May 2011, pp. 195–200.

[21] A. J. Ganesh, A. Kermarrec, and L. Massouli, "Peer-to-peer membership management for gossip-based protocols," *IEEE Transactions on Computers*, vol. 52, no. 2, pp. 139–149, Feb. 2003.

[22] S. Voulgaris, D. Gavidia, and M. Van Steen, "Cyclon: Inexpensive membership management for unstructured p2p overlays," *Journal of Network and Systems Management*, vol. 13, no. 2, pp. 197–216, Jun. 2005.

[23] B. Pretre, "Attacks on peer-to-peer networks," Ph.D. dissertation, Swiss Federal Institute of Technology (ETH), 2005.

[24] M. Brinkmeier, G. Schfer, and T. Strufe, "Optimally dos resistant p2p topologies for live multimedia streaming," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 6, Jan. 2009.

[25] S. V. Buldrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, pp. 1025–1028, Apr. 2010.

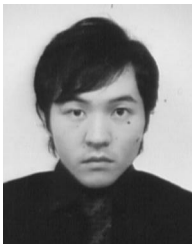
[26] T. Tanizawa, "Percolation on correlated complex networks," *Computer Software-JSSST*, vol. 28, no. 1, pp. 135–144, Feb. 2011.

[27] Y. Matsumoto, "Ruby [Online]." Available: http://www.ruby-lang.org/en/.

[28] S. Sun, Z. Liu, Z. Chen, and Z. Yuan, "Error and attack tolerance of evolving networks with local preferential attachment," *Physica A: Statistical and Theoretical Physics*, vol. 373, no. 1, pp. 851–860, Jan. 2007.

[29] M. Molloy and B. Reed, "The size of the giant component of a random graph with a given degree sequence," *Combinatorics, Probability, and Computing*, vol. 7, no. 3, pp. 295–305, Sep. 2000.

[30] R. Albert and A.-L. Barabasi, "Statistical mechanics of complex networks," *Reviews of modern physics*, vol. 74, pp. 47–97, Jan. 2002.



Katsuya Suto received his B.E. in Information Engineering from Iwate University, Japan, in 2011. Currently, he is pursuing the M.S degree in the Graduate School of information Science (GSIS) at Tohoku University. His research interests are the area of P2P networks, content delivery/distribution networks, and network security. He is a student member of IEICE and IEEE.

Hiroki Nishiyama received his M.S. and Ph.D. in Information Science from Tohoku University, Japan, in 2007 and 2008, respectively. He was a Research Fellow of the Japan Society for the Promotion of Science (JSPS) until finishing his Ph.D, following which he went on to become an Assistant Professor at the Graduate School of Information Sciences at Tohoku University. He has received Best Paper Awards from the IEEE Global Communications Conference 2010 (GLOBECOM'2010) as well as the 2009 IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC'2009). He was also a recipient of the 2009 FUNAI Foundation's Research Incentive Award for Information Technology. His active areas of research include, traffic engineering, congestion control, satellite communications, ad hoc and sensor networks, and network security. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and an IEEE member.

Nei Kato received his M.S. and Ph.D. Degrees in information engineering from Tohoku University, Japan, in 1988 and 1991, respectively. He joined Computer Center of Tohoku University at 1991, and has been a full professor with the Graduate School of Information Sciences since 2003. He has been engaged in research on satellite communications, computer networking, wireless mobile communications, smart grid, image processing and neural networks. He has published more than 300 papers in peer-reviewed journals and conference proceedings. He currently serves as the Chair of IEEE Satellite and Space Communications Technical Committee, the Vice Chair of IEEE Ad Hoc & Sensor Networks Technical Committee, the Chair of the IEICE Satellite Communications Technical Committee, a technical editor of IEEE Wireless Communications (2006-), an editor of IEEE Transactions on Wireless Communications(2008-), an associate editor of IEEE Trans. on Vehicular Technology (2010-), an editor of IEEE Trans. on Parallel and Distributed Systems(2012-), co-guest-editor of several SIs in IEEE Wireless Communications Magazine. He has served as a symposium co-chair of GLOBECOM'07, ICC'10, ICC'11, ICC'12, Vice Chair of IEEE WCNC'10, WCNC'11, ChinaCom'08, ChinaCom'09, Symposia co-chair of GLOBECOM'12, and workshop co-chair of VTC2010. His awards include Minoru Ishida Foundation Research Encouragement Prize(2003), Distinguished Contributions to Satellite Communications Award from the IEEE Communications Society, Satellite and Space Communications Technical Committee(2005), the FUNAI information Science Award(2007), the TELCOM System Technology Award from Foundation for Electrical Communications Diffusion(2008), the IEICE Network System Research Award(2009), KDDI Foundation Excellent Research Award (2012), and IEEE GLOBECOM Best Paper Award(Twice). Besides his academic activities, he also serves on the expert committee of Telecommunications Council, Ministry of Internal Affairs and Communications, and as the chairperson of ITU-R SG4 and SG7, Japan. Nei Kato is a Distinguished Lecturer of IEEE Communications Society(2012-2013) and the PI of JSPS A3 Foresight Program(2011-2014).

Takayuki Nakachi received a Ph.D. degree in electrical engineering from Keio University, JAPAN in 1997. Since he joined NTT Laboratories in 1997, he has been engaged in research on Super High Definition (SHD) image and video coding, especially in the area of lossless and scalable coding. His current research interests include distributed source coding, audio-visual communications, super resolution and secure image processing. From 2006 to 2007, he was a visiting scientist at Stanford University, USA. In 2010, He received a 26th TELECOM System Technology Award. He served as an associate editor of IEICE Transaction Fundamentals and Fundamentals Review from 2005 to 2010 and from 2009 to 2011, respectively. He currently serves as the ITC-CSCC2012 Technical Program Committee Co-Chair and a member of IEEE ISPACS International Steering Committee. He is currently a senior research engineer of media processing systems research group in NTT Network Innovation Laboratories. He is a member of IEICE and IEEE.

Tatsuya Fujii received his B.S., M.S. and Ph.D. degrees, all in electrical engineering from the University of Tokyo, Tokyo, Japan, in 1986, 1988, and 1991, respectively. He joined NTT, Japan, in 1991. He has been researching parallel image processing and super-high-definition image communication networks. In 1996, he was a visiting researcher of Washington University in St. Louis. He was a director of digital cinema developing project, and is currently a group leader of media processing systems research group in NTT Network Innovation Laboratories. He is a member of IEICE, ITE of Japan and IEEE.

Atsushi Takahara received the B.S., M.S., and Dr. of Engineering degrees from Tokyo Institute of Technology in 1983, 1985, and 1988, respectively. He joined NTT LSI Laboratories in 1988 and has been researching formal methods of VLSI design, reconfigurable architectures, and IP processing. From 2003 to 2008, he was the director of Service Development & Operations Department, Visual Communications Division, NTT Bizlink Inc to develop and operate an IP-based visual communication service. From 2008 to 2011, he was the Executive Manager of Media Innovation Laboratory in NTT Network Innovation Laboratories. Since 2011, he has been the Director of NTT Network Innovation Laboratories. His current research interests are in IP networking for real time communication applications and IP infrastructure technologies. He is a member of IEEE, ACM, IEICE, and IPSJ.