NRIT: Non-Redundant Indirect Trust Search Algorithm for a Cross-Domain based CDNi-P2P Architecture

Shi Li, Inshil Doh, Kijoon Chae

Department of Computer Science and Engineering, Ewha Womans University, Korea

lishi1116@ewhain.net, isdoh1@ewha.ac.kr, kjchae@ewha.ac.kr

***Abstract*—A content delivery network (CDN), as a distributed network architecture, enhances efficient delivery of content. The interconnection of different CDNs (CDNi) further improves efficiency and the experience of end users. As another distributed network with high availability and high performance, a peer-to-peer (P2P) network can provide efficient resource sharing. To combine the advantages of the two networks, we propose a hybrid CDNi-P2P architecture, along with trust management models to achieve more efficient content delivery. In CDNi-P2P architecture, end users can obtain the requested content from the nearest CDN edge server, and can also share these contents with other users in the same domain as a P2P network. After the transactions, users can rate each other based on the reputation evaluation method adopted in the system. For some mobile users, they can move among different domains and share the contents who have with the end users in different system. In general, different systems adopt different reputation evaluation standards. This leads to disparate trust values for mobile users in different systems. Based on the architecture, we propose two trust models to solve this problem: a local trust model and a cross-domain trust model. To evaluate reputation more effectively and accurately, we also propose a search algorithm for the trust model called the non-redundant indirect trust search algorithm (NRIT-SA). Using the proposed trust models, a mobile user can transform his/her local trust into mobile trust in a new domain. We thus avoid disparate trust values for a single user in different domains and improve the availability of the content possessed by mobile users as they move among different domains. The result of the performance analysis shows that when there is a high connectivity degree of users in the system, the calculation time of the proposed NRIT-SA tends to be stable. And depending on the comparison result with the full search algorithm, NRIT-SA shows more efficient calculation performance and more reliable result.**

***Keyword*—CDNi, Cross Domain, Mobile, Reputation Evaluation, Trust**

Manuscript received on November 25, 2016. This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (2016R1A2B4015899), and a follow-up the invited journal to the outstanding paper of the 19th International Conference on Advanced Communication Technology (ICACT 2017). It is also partially supported by the State Scholarship Fund organized by the China Scholarship Council (CSC).

Shi Li is with the Computer Science and Engineering Department, Ewha Womans University, Seoul, 03760 Korea (e-mail: lishi1116@ewhain.net).

Inshil Doh is with the Computer Science and Engineering Department, Ewha Womans University, Seoul, 03760 Korea (e-mail: isdoh1@ewha.ac.kr).

Kijoon Chae is with the Computer Science and Engineering Department, Ewha Womans University, Seoul, 03760 Korea. He is the corresponding author of this paper. (Corresponding author phone: +82-2-3277-2370; fax: +82-2-3277-3506; e-mail: kjchae@ewha.ac.kr).

I. INTRODUCTION

TWO major technologies provide large-scale video streaming over the Internet: content delivery networks (CDNs) and peer-to-peer (P2P) networks. Both of them can distribute content with high availability and high performance. With CDNs, an origin server distributes content to cache servers (edge servers) located close to end users, resulting in fast, reliable applications and Web services for users [1]. There are many commercial CDN companies: Akamai, AT&T, NTT Communication, Limelight, Mirror Image, Level 3, etc. In practice, it is extremely expensive to deploy and maintain CDN servers, so CDN architectures do not benefit from high scalability. On the other hand, P2P networks can be highly scalable because of their low start-up costs and because they rely on peers instead of dedicated and expensive servers. The complementary advantages of CDN and P2P networks allow their combination into a hybrid CDN-P2P architecture that creates a distribution system with higher scalability and reliability than either kind of network alone [2], [3].

Content delivery network interconnection (CDNi) is a new interactive network infrastructure that allows information and content to be transmitted between different CDNs through specific interfaces. CDNi provides all of the benefits of CDN and also has some unique characteristics. In CDNi, end users do not need to register at all CDN providers to obtain content from different content service providers (CSPs). When requested content is not cached in any edge server of the registered CDN, the end-user's request will be redirected to other CDNs to capture the content through the interfaces among them. (CDNi requires the specification of interfaces and mechanisms to address issues such as request routing, distribution metadata exchange, and log in information exchange across CDNs [4].) As a result, content can be delivered via a CDN chain and transmitted to end users by the closest CDN. CDNi thus uses two categories of CDNs: the one that caches content from a CSP is called the upstream CDN (uCDN), and the one that delivers content directly to an end user is called the downstream CDN (dCDN).

To deliver content more efficiently, we combine CDNi and P2P architectures into a hybrid CDNi-P2P network that combines the advantages of both, which can be found in our previous research as well [11]. Based on the the hybrid CDNi-P2P architecture, end-users could receive content from the

closest edger server of the dCDN with which they are registered and from peers in the same domain.

In a hybrid CDNi-P2P network, all the end users, as peers, are both consumers and providers. When an end-user requests content from a peer, some users might be honest and provide accurate content received from the edge server of a dCDN, others might be self-serving and unwilling to provide content to peers, and still others might be malicious and provide false or harmful content [5]. A trust model provides a way to generate trust based on a peer's history of behavior [6]-[10]. A larger trust value indicates a higher probability of providing accurate content. Meanwhile, some mobile peers move among different systems or domains. From a reputation-estimation point of view, they need to develop a trust value in each P2P system. In general, different P2P systems and domains adopt different trust models and reputation evaluation standards that lead to disparate trust values for a single peer in different domains, even if that user always has the same performance. Most research on existing reputation systems focuses on the trust model of a single system or domain. Creating a cross-domain trust model has never been considered. Therefore, in this paper, we propose a cross-domain trust model for a hybrid CDNi-P2P network. And based on this cross-domain trust model, a non-redundant indirect trust search algorithm is proposed in this paper as well, which can be used to calculate the local trust degree more efficiently and more reliably.

The rest of this paper is organized as follows: we introduce our local trust model in Section 2 and propose our hybrid CDNi-P2P architecture and cross-domain trust model in Section 3. And the performance analysis and conclusion are in Section 4 and Section 5, respectively.

II. Proposed Local Trust Model

A cross-domain trust model presupposes a relative reputation evaluation for each participant in a local system, which can indicate the reliability of each individual participant. In this section, we propose a local trust model to generate a relative reputation value for each participant according to the different reputation evaluation standards currently used by local systems.

A. Trust Value and Trust Degree

Existing online reputation systems and research use two main approaches to evaluate a participant's reputation within a specific network. In the first approach, the ratings for both the service receiver and provider are given via a bi-directional or one-directional rating after each transaction. The rating could take the form of reputation scores, feedback ratings, positive feedback rates, etc. The overall reputation of a participant is the sum of those ratings and is called that user's *trust value*, denoted by *v*. Online reputation systems that use this approach are the online auction system eBay, Amazon, and Alibaba. Generally, the trust value is an integer equal to or greater than zero that is public to all system participants; other participants can decide whether to trust a participant based on this trust value. In the second approach, both the service receiver and provider can rate each other after a transaction, and they calculate the *trust degree* to the others [6-10]. The trust degree is a value between 0 and 1, denoted by *d*. For example, when there are two participants *i* and *j*, *i* can rate *j* after each transaction, and the trust degree of *i* trusting *j* (denoted by d_{ij}) is the ratio of positive ratings. The relations among those evaluations can be illustrated by a graph called a reputation evaluation diagram.

B. Local Trust Model

The objective of a local trust model is to calculate the relative reputation degree (*local trust degree*) of each participant in a local system using a value between 0 and 1. According to the two approaches explained above, we propose two methods to calculate the local trust degree of an individual participant. Fig. 1 illustrates the two types of reputation systems: the *trust value* reputation system and the *trust degree* reputation system.

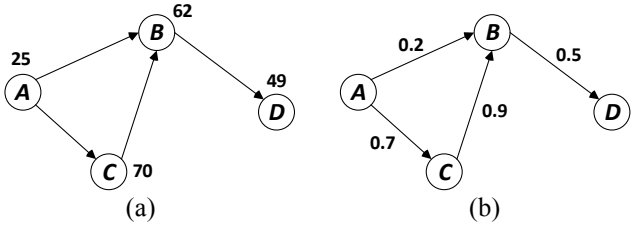

Fig. 1. (a) Trust value reputation system. (b) Trust degree reputation system.

1) Trust Value Reputation System

We assume there are *n* participants in the system, and each participant *i*, here $i \in (1, n)$, has a trust value v_i which is derived from the ratings given by other participants after the transactions in a trust value based reputation system. Thus, the local trust degree of *i* can be calculated as follows:

$$local\_d_i = \frac{v_i}{max_{j\in(1,n)}\, v_j} \quad (1)$$

Here, $local\_d_i$ is a value between 0 and 1 that indicates the ranking of *i*'s trust value in the system. Thus, as shown in Fig. 1 (a), the local trust degree of *D* $local\_d_D$ is 0.7 according to equation (1).

2) Trust Degree Reputation System

To calculate the local trust degree of participant *j* in trust degree reputation system, we first need to obtain the trust degrees of all the other participants trusting in *j*, i.e., we need all d_{ij}, $i \in (1, n)$, which can be calculated as follows:

$$d_{ij} = \sum_{k=1,k\neq i,k\neq j}^{n} d_{ik}\, d_{kj} \quad (2)$$

Equation (2) is a recursive equation used in computing d_{ik} or d_{kj}. In Fig. 1 (b), d_{AD} can be calculated as $d_{AB}\times d_{BD} + d_{AC}\times d_{CD}$, and d_{CD} can be calculated as $d_{CB}\times d_{BD}$, i.e., $d_{AD} = d_{AB}\times d_{BD} + d_{AC}\times d_{CB}\times d_{BD} = d_{AB}\times d_{BD} + d_{AB}\times d_{BD}$. In other words, there are two ways to calculate d_{AB}: one results in the *direct trust degree*, and the other in the *indirect trust degree*. However, in a reputation evaluation system, direct trust will be more reliable than indirect trust. Thus, if a trust degree can be calculated both ways (direct and indirect), the direct way will be selected. In this case, we use only the direct trust degree to calculate d_{AD}, whose result is 0.1. Similarly, we can calculate d_{BD} and d_{CD} as 0.5 and 0.45 respectively.

However, in a realistic reputation system, a large number of peers can communicate and rate one another; thus, a realistic reputation evaluation diagram is huge and complicated. There are many different paths from one peer to

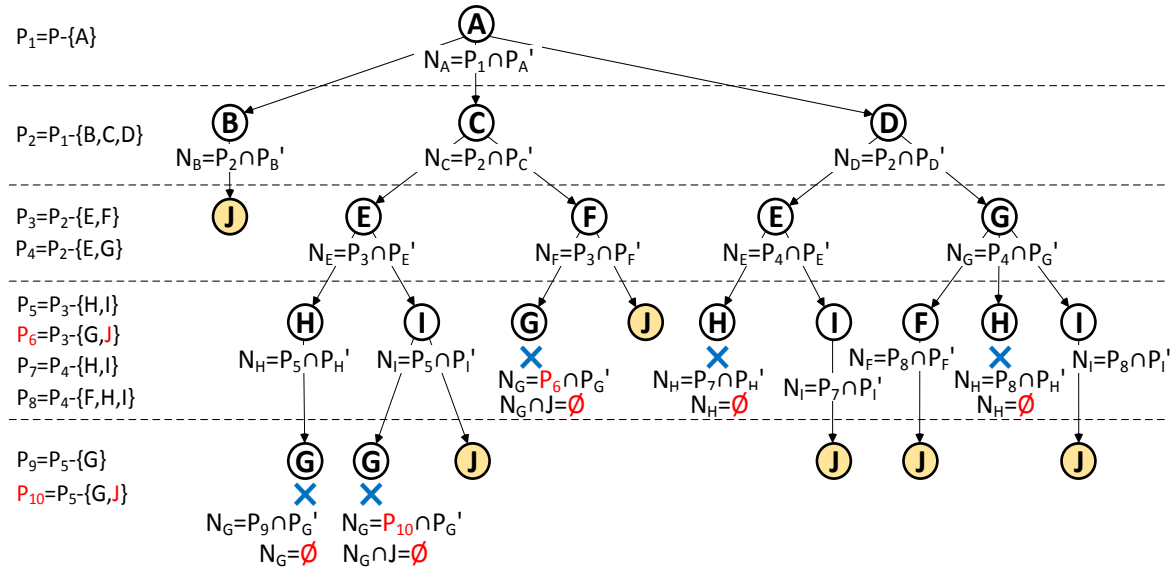

Fig. 3. The calculation process of the trust degree from p_A to p_J using NRIT-SA.

another, which makes it difficult to select a direct trust way among them. Moreover, the reputation evaluation diagram will contain some cycles, as shown in Fig. 2, which is a difficult issue for the indirect trust degree calculation, and most research has excluded it from consideration. In this paper, we propose an algorithm to calculate the indirect trust degree by considering the cycles and excluding redundancies when there is direct trust. We call it the non-redundant indirect trust search algorithm (NRIT-SA).

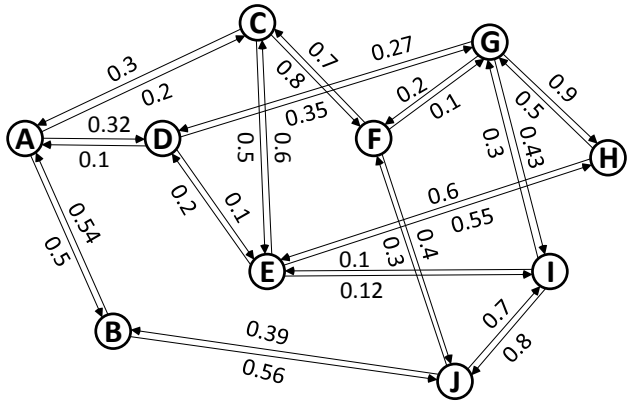

Fig. 2. Reputation evaluation diagram.

We assume that a P2P evaluation system contains n peers, and each peer k can be considered as a point in the reputation evaluation diagram, which is denoted p_k, $k \in (1, n)$. If peer k evaluates peer l after a transaction between them, an arrow is generated from k to l in the diagram, denoted $arr_{k,j}$. Thus, the reputation evaluation diagram composed of the point set $\boldsymbol{P} = \{p_k\}$, $k \in (1, n)$, and the arrow set $\boldsymbol{ARR} = \{arr_{k,j} \mid k, j \in (1, n)$ and $k \neq j\}$. $\forall\, p_k \in \boldsymbol{P}$, $\exists\, \boldsymbol{P}_k$', which is a set of points that p_k can indicate in the reputation evaluation diagram. As shown in Fig. 2, $\boldsymbol{P}_C' = \{p_A, p_E, p_F\}$. Moreover, if $\boldsymbol{P}_k' = \emptyset$, there is no point that p_k can indicate.

NRIT-SA is a breadth first search algorithm that does not search for the shortest path from source to destination. Its objective is to calculate the indirect trust degree using as much direct evaluation of others as possible. The reputation evaluation diagram shown in Fig. 2 is based on a trust degree reputation system. To calculate the indirect trust degree from p_A to p_J based on equation (2) and exclude redundant and cyclic evaluations, the NRIT-SA algorithm can search the indirect evaluation paths, as shown in Fig. 3.

Step 1: First, as a source point, p_A should select a set of points as its next step, denoted $\boldsymbol{N}_A$. As shown in Fig. 2, a point set $\boldsymbol{P}_A'$ contains all the points that p_A can indicate, here $\boldsymbol{P}_A' = \{p_B, p_C, p_D\}$. To avoid a redundant path, p_A should remove itself from the available point set $\boldsymbol{P}$ and generate a new point set $\boldsymbol{P}_1 = \boldsymbol{P}\text{-}\{p_A\}$ that can be used instead of $\boldsymbol{P}$ in the next step. Then, the next step point set of p_A can be calculated as $\boldsymbol{N}_A = \boldsymbol{P}_1 \cap \boldsymbol{P}_A' = \{p_B, p_C, p_D\}$. NRIT-SA will move to each of the next step points of p_A to continue. If there is a $p_i \in \boldsymbol{N}_A$ as the destination point, then there is a direct evaluation from the source to the destination peer, and the algorithm is complete because there is no need to calculate the indirect trust degree.

Step 2: To avoid a redundant path, the available point set $\boldsymbol{P}_1$ should remove each point p_i that belongs to set $\boldsymbol{N}_A$ (i.e., $p_i \in \boldsymbol{N}_A$) to generate the newly available point set $\boldsymbol{P}_2$. In this case, $\boldsymbol{P}_2 = \boldsymbol{P}_1\text{-}\{p_B, p_C, p_D\}$. $\forall\, p_i \in \boldsymbol{N}_A$ will calculate its next step point set by $\boldsymbol{N}_i = \boldsymbol{P}_2 \cap \boldsymbol{P}_i'$. If $\boldsymbol{N}_i = \emptyset$, there is no point that p_i can indicate, and the search from p_i will be stopped. And if $\boldsymbol{N}_i \cap p_J = \emptyset$ (here p_J indicates the destination point), a direct trust way has already been found in the previous step p_i to the destination point, so the search from p_i will be stopped. If $\boldsymbol{N}_i = p_J$, then the path from the source to the destination should be recorded as one of the NRIT paths. For the other cases of $\boldsymbol{N}_i$, NRIT-SA will move to each of the next step points of p_i and repeat the similar process in Step 2.

After finding all of the NRIT paths from a source point to a specific destination using NRIT-SA, the trust degree from the source point to the destination can be calculated using Equation (2). In the example shown in Fig. 3, the trust degree d_{AJ} can be calculated using all the NRIT paths: $d_{AB} \times d_{BJ} + d_{AC} \times d_{CE} \times d_{EI} \times d_{IJ} + d_{AC} \times d_{CF} \times d_{FJ} + d_{AD} \times d_{DE} \times d_{EI} \times d_{IJ} + d_{AD} \times d_{DG} \times d_{GF} \times d_{FJ} + d_{AD} \times d_{DG} \times d_{GI} \times d_{IJ}$. Similarly, we can also calculate the trust degrees from all the other points to this destination. According to the trust degrees of j given by all the other participants in the system, the local trust degree of

participant *j* can be calculated as follows:

$$local\_d_j = \frac{\sum_{i=1, i\neq j}^{n} d_{ij}}{n-1} \quad (3)$$

Here, *n* indicates the number of participant peers in the system, and $local\_d_j$ is a value between 0 and 1 that represents the average trust ranking for peer *j* based on the ratings given by all the other participants in the system.

III. Proposed Cross-Domain Trust Model for Hybrid CDNi-P2P Network

From a reputation estimation point of view, mobile peers who move among different systems or domains need trust values in each P2P system. In general, different P2P systems or domains adopt different trust models and reputation evaluation standards. That leads to disparate trust values for a single peer in different domains, even if the user always offers the same performance. In this section, we propose a cross-domain trust model for a mobile peer in a hybrid CDNi-P2P network.

A. Hybrid CDNi-P2P Network Architecture

Our proposed hybrid CDNi-P2P network architecture is shown in Fig. 4. The architecture contains two types of CDNs: uCDNs and dCDNs. Content provided by CSPs is stored only in the edge servers of the uCDNs. For an end user u_1 who can only obtain service directly from dCDN-A (i.e., the end user u_1 registers at dCDN-A), if u_1 sends a content request to the origin server, the content will be delivered from the uCDN to dCDN-A and then transmitted to the end-user through the closet edge server of dCDN-A. If another end-user from the same domain also wants to obtain this content, s/he can get the content directly from u_1. In this situation, each CDN can act as an uCDN and dCDN simultaneously based on the content requested by the end-user.

B. Cross-Domain Trust Model

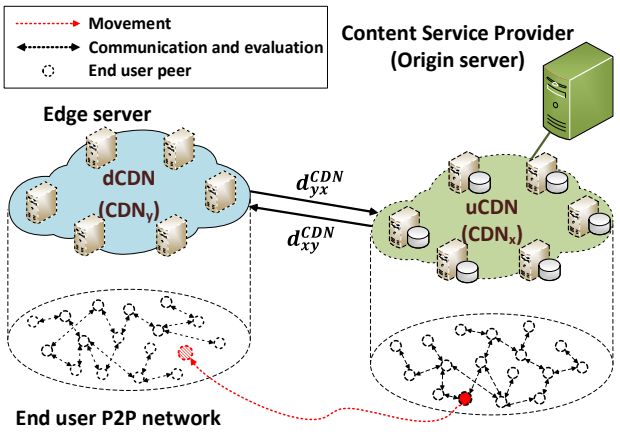

Fig. 4. Hybrid CDNi-P2P network architecture.

In Fig. 4, a mobile end user peer (the red solid point) can move between uCDN and dCDN domains. Some mobile peers with high trust values in one P2P domain could have their trust values initialized based on the trust model used in a new domain when they move because they are new-comers to the new domain. This will lead to a waste of resources, because other peers are unwilling to obtain content from a new peer. The mobile peer must wait a long time to accumulate trust in the new domain.

We assume that the uCDN and dCDN can also rate each other after each transaction between them, and that their evaluation method is based on the trust degree reputation system described in Section 2. We denote the two CDNs as CDN_x and CDN_y respectively. The trust degree that CDN_x gives CDN_y is d_{xy}^{CDN}, and the trust degree that CDN_y gives CDN_x is d_{yx}^{CDN}. When a mobile user u_m would like to move from CDN_x to CDN_y, u_m will send a mobile request message to CDN_x in order to obtain the individual local trust degree from CDN_x where u_m registered before. Because CDN_x could collect the trust information of all users located in its domain periodically, it can calculate a fair and credible local trust degree for each user. After receiving the mobile request message, CDN_x will calculate the local trust degree of u_m indicated as $local\_d_{u_m}^{CDN_x}$ by using the local trust model proposed above, and deliver $local\_d_{u_m}^{CDN_x}$ to CDN_y. If it is the first time for mobile user u_m to move from CDN_x to CDN_y domain, the *mobile trust degree* of u_m can be calculated by CDN_y as follows:

$$mobile\_d_{u_m}^{CDN_x \to CDN_y} = local\_d_{u_m}^{CDN_x} \times d_{yx}^{CDN} \quad (4)$$

Here, it should be noted that the trust degree between CDNs indicates how CDN_y rates CDN_x. If u_m already has a trust value (or trust degree) in CDN_y, it is used continuously.

If CDN_y is a trust value reputation system and the number of total participants is *t*, the *mobile trust degree* of u_m can be transformed to the trust value in CDN_y as follows.

$$v_{u_m}^{CDN_y} = mobile\_d_{u_m}^{CDN_x \to CDN_y} \times max_{j\in(1,t)} v_j^{CDN_y} \quad (5)$$

And if CDN_y is a trust degree reputation system, the *mobile trust degree* of u_m can be the trust degree in CDN_y for all other participants.

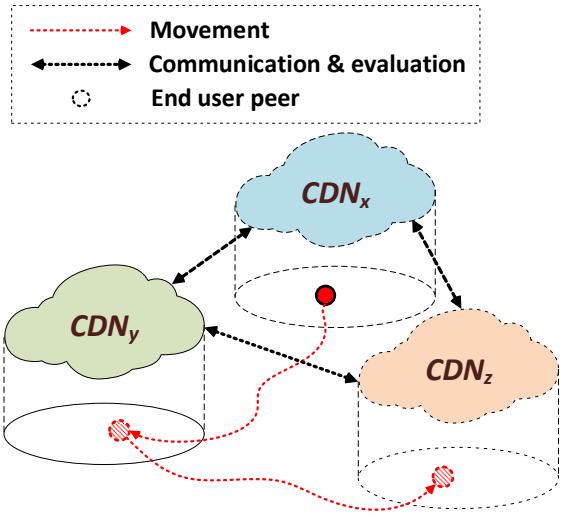

Fig. 5. A mobile user movement scenario.

In the new domain CDN_y, the mobile user u_m can register at CDN_y and receive contents from CDN_y, then share the contents with other users in the new domain. And the calculated trust value or trust degree which is derived from $mobile\_d_{u_m}^{CDN_x \to CDN_y}$ will be used as the initial evaluation value to all the other users located in CDN_y. And it can be

updated depending on the ratings given by the other users after transactions.

Moreover, there are some special cases during the mobile user moves among CDNs in this CDNi-P2P hybrid network, which are listed as follows. Depending on these cases, we will discuss the different applications of proposed cross-domain trust model. First, we need to define some terminologies. Take the figure shown in Fig. 5 as a scenario, a mobile user located in CDN_x moves to CDN_y domain, later, this user leaves CDN_y and moves to another CDN_z domain. In this scenario, CDN_x, CDN_y, CDN_z are called *original CDN*, *intermediate CDN* and *destination CDN*, respectively.

1) No transaction with destination CDN

In this case, the destination CDN has never exchanged contents with the original/intermediate CDN before, thus there is no direct evaluation between these two CDNs. In order to calculate the mobile trust degree of user as shown in Equation (4), the destination CDN will ask its internet service provider (ISP), which can be considered as the manager of CDN, for the indirect evaluation to the original/intermediate CDN. And by using the proposed NRIT search algorithm, the ISP can generate the indirect trust degree that destination CDN trusts in other CDNs. Depending on it, the destination CDN can calculate the mobile trust degree of the mobile user.

2) No transaction with other users in intermediate CDN

If the mobile user does not communicate with any other users in the new domain, its trust value or trust degree will not be changed. When s/he moves to another domain called CDN_z, s/he does not need to calculate the new local trust degree in the intermediate CDN_y domain. Instead, the local trust degree calculated in the original CDN_x domain can be used, because there is not any new evaluation given by the users in intermediate CDN_y, and we believe that the local trust degree calculated in the original CDN_x is more credible which is based on the actual transaction of this mobile user. Then, the mobile trust degree of this user can be calculated depending on the Equation (4), here d_{zx}^{CDN} is used as the trust degree that CDN_z trust in CDN_x. And if there is no direct transactions between CDN_x and CDN_z, the method introduced in the first case can be referred.

3) Trust value or Trust degree updated in intermediate CDN

If the mobile user communicates with other users and be evaluated in the intermediate CDN_y domain, the trust value or trust degree will be updated. When s/he would like to move to another domain called CDN_z, a new local trust degree in CDN_y needs to be calculated depending on the local trust model proposed in this paper. And based on the Equation (4) and this new local trust degree, another mobile trust degree from CDN_y to CDN_z can be computed, which will be used by CDN_z to generate the initial evaluation value of this mobile user in the CDN_z domain.

IV. Performance Analysis

In this section, we will analyse performance of the proposed NRIT search algorithm, and compare it with one of the most well-known search algorithms called *full search algorithm*.

A. Calculation Time of NRIT-SA

Based on the proposed algorithm NRIT-SA, mobile users can calculate their local trust degree which is mainly dependent on the direct evaluations among users in the local system. The proposed NRIT-SA can eliminate all the redundant indirect connections between two users, if there is the direct evaluation between them. Because we believe the fact that the direct evaluation is more trustworthy than the indirect one. Moreover, for users who cannot provide the direct evaluation to a specific user, i.e. these users have never conduct a transaction before, the indirect evaluation from others can also be used to generate the trust degree to the specific user. Thus, the connectivity rate among users become a significant determinant of the performance in NRIT-SA.

In this section, we will discuss the relationship between the connectivity rate of users and the calculation time of the proposed algorithm. First, we will give the definition of the connectivity rate, here it is called *connectivity degree*, as follows.

Definition 1 (*Connectivity degree*)

For a local system with n users, the connectivity degree can be calculated by

$$d_{connectibity} = \frac{\sum_{i=1}^{n}\sum_{j=1,j\neq i}^{n}\lceil direct\_d_{ij}\rceil}{n(n-1)} \quad (6)$$

Here, $direct\_d_{ij}$ indicates the direct trust degree between user u_i and u_j, which can be considered as the direct connection between node u_i and u_j in Fig. 2. From the definition, we know that the connectivity degree indicates the percentage of real connections among users in a local system. According to this definition, we will analyze the relationship between the calculation time of proposed algorithm NRIT-SA and the connectivity degree of users in a local system.

The tool we use to implement NRIT-SA is JDK 1.7.0_80, and 3.60GHz processor with 64-bit OS. The connections among users are randomly selected based on the connectivity degree. For two specific user u_i and u_j, the time to calculate the trust degree d_{ij} based on NRIT-SA is shown in Fig. 6.

In Fig. 6, the calculation time indicates the average value of processing time based on different connection topologies which is randomly generated. From the figure, we can see that the processing time of NRIT-SA increases along with the growth of the number of users in the system. And when there are 50 users, the longest calculation time is around 30s which can be tolerant by an evaluation system, because the calculation of trust degree d_{ij} is used for generating the local trust degree of mobile user u_j which can be considered as an offline value during a short period of time. The reason is that, for user u_j, its local trust degree $local\_d_j$ can be influenced by the change of other trust degree between any two users in the system, however, according to equation (2) and (3), this influence is negligible small when there are large numbers of users in the local system.

Moreover, from Fig. 6, we can see that, for different number of users, the peak values of calculation time typically appear around 20% of connectivity degree. And along with the increase of connectivity degree, NRIT-SA processing time decreases exponentially. When the connectivity degree increases to 40%, all the calculation time is around 1s.

According to a well-known fact that the number of system users will tend to be stabilized, the connectivity degree will increase with time, thus the calculation time of proposed algorithm can also tend to a small and stable value.

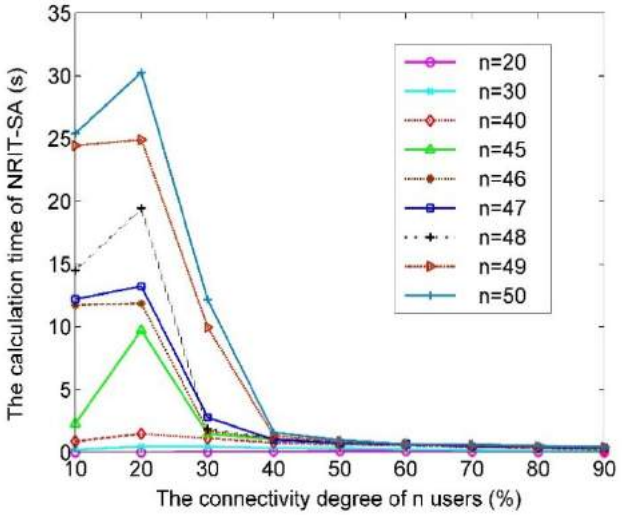

Fig. 6. The calculation time of NRIT-SA based on different connectivity degree of the *n* users.

B. Comparison with Full Search Algorithm

Moreover, as a well-known search algorithm, *full search* is widely used in the search mechanism. And it is also employed in some famous reputation evaluation systems. Then, we will compare our NRIT-SA with the full search algorithm, and the definition of the *full search* is as follows.

Definition 2 (*Full search*)

For each individual user *j* located in a system, the trust degree of other users trust in user *j* is calculated only by the Equation (2), i.e. the trust degree is contributed from both *direct trust degree* and *indirect trust degree*.

The definition of full search implies that all users in the system needs to participant in the calculation of trust degree between any two users. In order to generate a new trust degree, full search algorithm should refer to more indirect trust degree. Thus, the full search algorithm will generate a larger trust degree than our NRIT-SA, which cannot be regarded as a more accurate result when compare with NRIT-SA, because we believe that the direct trust degree is more trustworthy than the indirect one during P2P communications. Meanwhile, by using full search algorithm, it will take much more calculation time to search for all paths from the source node to the destination node. The comparison of the calculation time between full search algorithm and the proposed NRIT-SA is illustrated in Fig. 7 as follows.

Depending on the result shown in Fig. 6, we know that if the connectivity degree is more than 40%, the calculation time of NRIT-SA tend to be stable. Thus, the result illustrated in Fig. 7 is based on the 40% connectivity degree of users in the domain. From Fig. 7, we can see that the calculation time of NRIT-SA is less and be stable along with the increase of the number of users. However, the calculation time of full search algorithm exponentially increase when the number of users increases linearly. And even when there are only 15 users in the domain, the calculation time of full search algorithm is almost around 23s, which is much more than the time taken by the proposed NRIT-SA. Thus, depending on the result shown above, our NRIT-SA is much more efficient than the well-known full search algorithm.

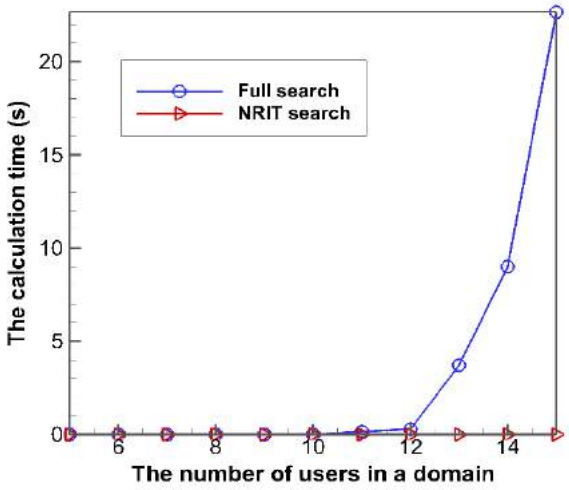

Fig. 7. The comparison of calculation time between full search algorithm and NRIT-SA when connectivity degree is 40%.

Moreover, because full search algorithm refers to more trust degrees existed in the system than NRIT-SA, any change of direct trust degree between two users will influence the calculation result of indirect trust degree among other users in the system. As an example shown in Fig. 8, we would like to calculate the indirect trust degree that user *A* trust in user *D* which is indicated as d_{AD}, and the trust degree between user *B* and *C* is different in Fig. 8 (a) and (b). Thus, based on the topology and the different values of d_{BC} shown in Fig. 8 (a) and (b), we will compare the influence on the calculation result of d_{AD} by using full search algorithm and NRIT-SA separately.

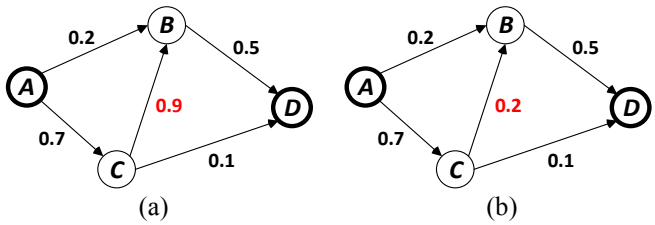

Fig. 8. An example of trust degree changes between two users.

First, depending on the full search algorithm, the trust degree that *A* trust in *D*, indicated as d_{AD}^{full}, can be calculated as $d_{AD}^{full} = d_{AB}\times d_{BD} + d_{AC}\times d_{CB}\times d_{BD} + d_{AC}\times d_{CD}$. And based on this formula, the result of d_{AD}^{full} is 0.485 and 0.24 in Fig. 8 (a) and (b) respectively. From these results, we know that the change of trust degree d_{CB} can lead to a distinct change of d_{AD}^{full}. Second, according to the proposed NRIT-SA, the trust degree that user *A* trust in user *D* is indicated as d_{AD}^{NRIT}, which can be calculated as $d_{AD}^{NRIT} = d_{AB}\times d_{BD} + d_{AC}\times d_{CD}$. And depending on this formula, the values of d_{AD}^{NRIT} are the same in Fig. 8 (a) and (b), which equal to 0.17. From the results shown above, we can see that the change of trust degree d_{CB} will not impact the calculation result of d_{AD}^{NRIT}. In other words, for the calculation of indirect trust degree d_{AD}^{NRIT}, the trust degree between user *B* and *C* is a uncorrelated value, which

changes cannot influence the result of d_{AD}^{NRIT}. In reality, the trust between two users should not be affected greatly by the trust among any other users. In other words, it is undesirable that the trust between two users is strongly correlated to some uncorrelated trust values of others. As a result, depending on the analysis above, it shows that the proposed NRIT-SA is more conform to the reality than the full search algorithm.

V. Conclusion

In this paper, we propose a hybrid CDNi-P2P architecture, an NRIT search algorithm, and two trust models: a local trust model and a cross-domain trust model. Based on the proposed NRIT-SA and trust models, a user can calculate his/her local trust more effectively and accurately, and a mobile user can transform his/her local trust into mobile trust that can be taken to and used in a new domain. The proposed models can avoid disparate trust values for a single user in different domains and improve the availability of content possessed by mobile users as they move among different domains. And from the performance result, we know that the peak value of the calculation time appears around 20% of connectivity degree, and along with the increase of the connectivity degree, the calculation time will decreases exponentially. And when the connectivity degree is more than 40%, the calculation time tends to be stable, which value is around 1s. From the comparison result with the full search algorithm, we can see that our NRIT-SA shows more efficient calculation performance and more reliable indirect trust result. In the future, we will research more available cross-domain trust models for different network architectures.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (2016R1A2B4015899). It is also partially supported by the State Scholarship Fund organized by the China Scholarship Council (CSC). Kijoon Chae is the corresponding author of this paper.

References

[1] G. Pallis, A. Vakali, Insight and Perspectives for Content Delivery Networks. *Communications of the ACM*. 2006, **49** (1): 101-106.

[2] D. Xu, S. S. Kulkarni, C. Rosenberg, and H. K. Chai, Analysis of a CDN-P2P Hybrid Architecture for Cost Effective Streaming Media Distribution. *Multimedia Systems*. 2006, **11**: 383-399.

[3] H. Yin, X. Liu, T. Zhan, V. Sekar, F. Qiu, C. Lin, H. Zhang, and B. Li, Design and deployment of a hybrid CDN-P2P system for live video streaming: Experiences with LiveSky. *Proc. of the 17th ACM international conference on Multimedia*. 2009, pp. 25-34.

[4] L. Peterson, B. Davie, Framework for CDN Interconnection draft-ietf-cdni-framework-08. *Internet draft in Network Working Group of Internet Engineering Task Force (IETF)*. 2014.

[5] David Hales, Bruce Edmonds, Applying a Socially Inspired Technique (Tags) to Improve Cooperation in P2P Networks. *IEEE Trans. on Systems, Man, and Cybernetics-Part A: Systems and Humans*. 2005, **35** (3): 385-395.

[6] G. Zacharia and P. Maes, Trust management through reputation mechanisms. *Applied Artificial Intelligence*. 2000, **14** (9): 881–908.

[7] M. Richardson, R. Agrawal, and P. Domingos, Trust management for the Semantic Web. *Proc. of the Second International Semantic Web Conference*. 2003, pp. 351-368.

[8] S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina, The EigenTrust algorithm for reputation management in P2P networks. *Proc. of the Twelfth International World Wide Web Conference*. 2003, pp. 1-12.

[9] S.D.Ramchurn, N.R.Jennings, C.Sierra, and L.Godo, A computational trust model for multi-agent interactions based on confidence and reputation. *Proc.2nd Int. Joint Conf. on Autonomous Agents and Multiagent Systems (AAMAS)*, 2003, pp. 69-75.

[10] Y. Gil and V. Ratnakar, Trusting information sources one citizen at a time. *Proc. of the first International Semantic Web Conference*. 2000, pp. 162-176.

[11] S. Li, I. Doh, K. Chae, Non-Redundant Indirect Trust Search Algorithm Based on a Cross-Domain Trust Model in Content Delivery Network. *Proc. of the 19th International Conference on Advanced Communications Technology (ICACT)*. 2017.

Shi Li received the B.S. degree in the Department of computer science and engineering from Harbin Institute of Technology, China in 2010. She is currently a Ph.D. candidate in the Department of computer science and engineering at Ewha Womans University, Seoul, Korea. Her research interests include sensor network security, smart grid security and content delivery network security.

Inshil Doh received the B.S. and M.S. degrees in Computer Science at Ewha Womans University, Korea, in 1993 and 1995, respectively, and received the Ph.D. degree in Computer Science and Engineering from Ewha Womans University in 2007. From 1995-1998, she worked in Samsung SDS of Korea to develop a marketing system. She was a research professor of Ewha Womans University in 2009~2010 and of Sungkyunkwan University in 2011. She is currently an assistant professor of Computer Science and Engineering at Ewha Womans University, Seoul. Her research interests include wireless network, sensor network security, and M2M network security.

Kijoon Chae received the B.S. degree in mathematics from Yonsei University in 1982, an M.S. degree in computer science from Syracuse University in 1984, and a Ph.D. degree in electrical and computer engineering from North Carolina State University in 1990. He is currently a professor in Department of Computer Science and Engineering at Ewha Womans University, Seoul, Korea. His research interests are network security including sensor network, smart grid, CDN, SDN and IoT, and network protocol design and performance evaluation.