

The Bio-Networking Architecture **Bi-weekly report #12 (November 9, 2002): Distributed Discovery**

PI: Tatsuya Suda (suda@ics.uci.edu)

University of California, Irvine

<http://netresearch.ics.uci.edu/bionet/>

Introduction

In the Bio-Networking Architecture, a network application is implemented as a decentralized collection of autonomous cyber-entities called *cyber-entities*. One of the challenges with such a distributed framework is discovery of cyber-entities. Discovery provides the ability for applications to locate specific cyber-entities that may represent available services, information, or users.

In the bi-weekly report submitted on June 24, 2002, the PI described two new discovery mechanisms developed with support from DARPA. In this report, the PI focuses on evaluating performance of one of the two discovery mechanisms described in the report submitted on June 24, 2002. In the proposed mechanism, cyber-entity contains one keyword, and discovery involves locating cyber-entities that match the keyword. Cyber-entities also contain a limited set of relationships (links that include information about other cyber-entities) to other cyber-entities which they can communicate with. In this discovery algorithm, cyber-entities have limited transmission range. Hence they can build relationship only with other cyber-entities inside that range. These relationships between cyber-entities together form a network on which discovery queries are forwarded. The discovery mechanism in this report forwards discovery requests multiple hops and returns discovery hits along the same path.

Besides, in this discovery mechanism, PI exploits user's evaluation of the received discovery hits, which guide discovery request. User evaluation is defined as the user's degree of satisfaction with the returned hit, and allows the user to reward better hits from the discovery hits the user receives. This allows subsequent discoveries to obtain hits with greater user evaluation. To reflect user evaluation, each relationship is associated with a strength value for each keyword, which is called keyword strength. Keyword strength represents the usefulness of the relationship in discovering a cyber-entity that contains the given keyword and satisfied many users.

In this report, PI focuses on the behavior of the proposed discovery algorithm in static and dynamic environments. Dynamics in the environment in this report includes cyber-entity's random migration in the network. This migration makes relationship between cyber-entities dynamically vary because cyber-entities inside transmission range may go beyond the range, or new cyber-entity may go into the range. These dynamic properties impact how a discovery algorithm performs and may impact design choices for a discovery mechanism.

Proposed Discovery Algorithm

In this discovery mechanism, user evaluation guides discovery requests instead of flooding to all neighbors. Keyword strength summarizes information about user evaluation for each relationship partner's performance in the past discovery. Keyword strength is increased when the partner contributed to successful discovery that satisfied the user. In this case, a discovery hit isn't always issued from the partner. Even if the partner just forwarded the discovery hit returned by another cyber-entity, high user evaluation is given to the partner. On the contrary, keyword strength is decreased when the partner failed to return discovery hit or when the user wasn't satisfied with the discovery hit even if the partner succeeded in returning a discovery hit. Cyber-entities are informed of user evaluation for discovery hit by a reward message from the user, which is returned along the same path where a discovery request was originally forwarded. With this feedback mechanism, keyword strength dynamically changes according to user evaluation. Each cyber-entity probabilistically determines which partner it should forward discovery request

to on the basis of keyword strength. Therefore a discovery request is forwarded to the cyber-entity which has high user evaluation by high probability after some discovery processes are done in the network. Even if partners with high keyword strength migrate and go out of transmission range in dynamic environments, the cyber-entity probabilistically choose another partner smoothly. Accordingly this algorithm can also provide robustness to cyber-entity's mobility as a whole. Besides a cyber-entity also possesses self keyword strength, which determines whether to return discovery hit if the cyber-entity's keyword matches the discovery request. Self keyword strength changes dynamically according to user evaluation, which results in preventing useless cyber-entities from returning discovery hits. Consequently, this mechanism reduces the user's load to choose appropriate and useful information out of a bunch of hits.

How to calculate possibility out of keyword strength is critical in determining the behavior of discovery request. We proposed two methods for a cyber-entity to calculate probability for each cyber-entity to determine forwarding path of discovery request based on keyword strength. One method determines probability relatively by calculating the ratio of each partner's keyword strength to total of keyword strength of all partners. This is called "Rate" method. The other calculates probability absolutely with sigmoid function, which is called "Sigmoid" method.

Simulation Results

Simulations have been performed to evaluate the performance of the proposed discovery algorithm in static and dynamic scenarios. In this simulation, one cyber-entity is supposed to issue a discovery request with a keyword. Totally a discovery request is issued 5000 times. In static scenario, cyber-entities remain at the same position throughout. In dynamic scenario, each cyber-entity determines whether to migrate or stay every time a discovery request is issued. Figure 1 and 2 demonstrates user evaluation in static scenario comparing proposed algorithm and broadcast based algorithm. Figure 3 and 4 demonstrates user evaluation in dynamic scenario. Besides, to analyze difference between calculation methods, Rate method is used in Figure 1 and 3, and Sigmoid method is used in Figure 2 and 4. User evaluation is a value between 0(low) and 1(high), which indicates user evaluation for received discovery hits. We count 0 if there is no discovery hit and dotted averaged user evaluation of every 10 cycles in the graph.

In static scenario of Figure 1 and 2, user evaluation in the proposed algorithm is relatively low at initial cycles because random search is performed until keyword strength is accumulated enough in cyber-entities. Then user evaluation continues to go up and over the average of broadcast based algorithm after some cycles. This means that the proposed algorithm can adapt to the network by leaning the given network topology at the initial phase. To mention the difference of Rate and Sigmoid, there is more fluctuation in use evaluation of Figure 1 compared to Figure 2. That means Rate is more likely to fail in discovery even after keyword strength is accumulated enough. Rate always determines possibility to forward relatively. So if one cyber-entity has two or three partners that have high keyword strength, the possibility of forwarding will be diluted, which could result in no forwarding. On the other hand, Sigmoid determines possibility of forwarding absolutely, therefore dilution of possibility never happens.

In dynamic scenario of Figure 3 and 4, Rate's robustness to mobility is relatively low. On the contrary, Sigmoid proves its high robustness to mobility. By Sigmoid calculation, possibility increases in proportion to rise of keyword strength. Consequently multiple routes to more than one cyber-entities with good reputation are strengthened by user evaluation. Hence, even if one route is lost due to cyber-entity migration, other routes are still alive and guarantee high quality discovery. On the other hand, Rate calculation strengthens only one route to the best among some good cyber-entities. That is why Rate is relatively fragile to mobility.

User Evaluation in static scenario
comparing Rate and Broadcast

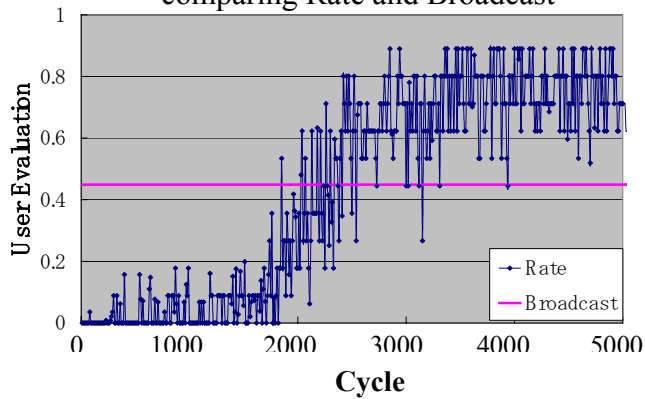


Figure1

User Evaluation in static scenario
comparing Sigmoid and Broadcast

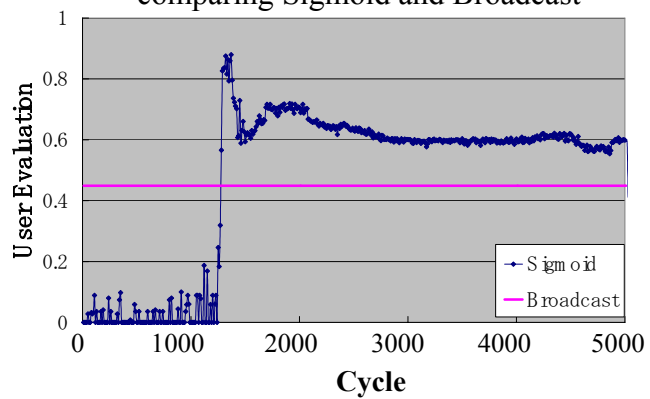


Figure2

User Evaluation in dynamic scenario
comparing Rate and Broadcast

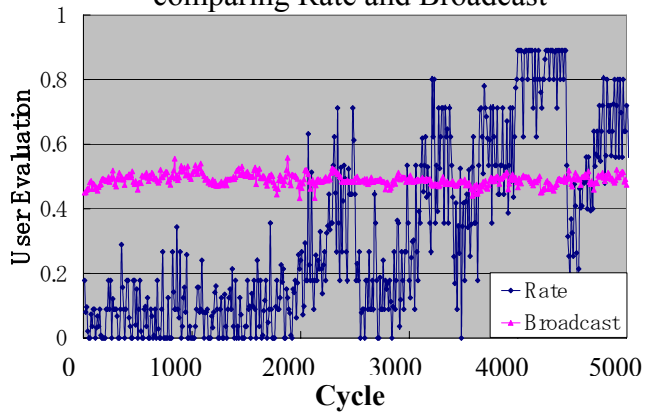


Figure 3

User Evaluation in dynamic scenario
comparing Sigmoid and Broadcast

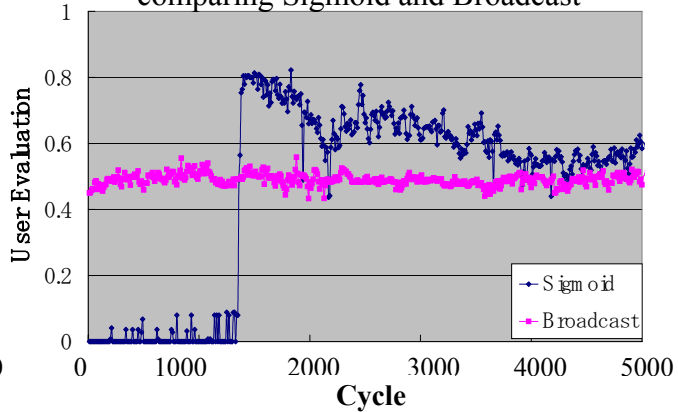


Figure 4