

The Escort Service Discovery Protocol

Richard Dunn
rdunn@cs.washington.edu

24 May 2002

Abstract

PiMP (The Pimpant Management Protocol), was a tremendous step forward in the management of Hoares. However, PiMP has been shown to only work effectively in the local area, with a small cluster of clients. Recently, much work has been performed in the arena of Escort Services, an attempt to generalize the work of Hoare Monitors to the wide area. We present an algorithm for discovering such services, and show that it optimally services clients in certain common cases.

1 Introduction

As stated in the author's previous work [1], much research has focused on the effective use of Hoare Monitors [2] in the management and marketing of Hoares. The Pimpant Management Protocol (PiMP) represented a great step forward, and was proved optimal under certain conditions. Unfortunately, no infrastructure existed to pair clients with Hoare Monitors, and thus the algorithm relied on clients being able to recognize the monitors. Despite having monitors adopt colorful accoutrements, this required clients to be in promiscuous mode, which unfortunately limited them to the local area.

In a groundbreaking work [3], Fleiss introduced the Escort Service, an attempt to generalize Hoare Monitors to the wide area. Establishing a distributed infrastructure meant that clients no longer had to be fully aware of all available Hoare Monitors; they could leverage an indexing service to successfully match them with available Hoares. Unfortunately, this simply shifted the problem from being able to find a Hoare Monitor to finding an Escort Service.

In traditional P2P systems, this bootstrapping is accomplished by establishing a set of well-known hosts. While in our domain well-known Hoares are common, the presence of the Common Operating Protocol Standard (COPS) implies that a new method must be used to discover Escort Services. In this paper we present the Escort Services Discovery Protocol, a client-based algorithm for performing this very task.

2 Algorithm Description

We suppose that a client, say Bob (B), wishes to utilize the services of Alice (A), who is registered with an Escort Service (S). B attempts the following:

First, B contacts an available semantic index, and searches on any of the following topics "Escort service", "Exotic Dance", "Massage", "Barney + Whipped Cream". While this method has the least cost, it also

has the largest chance of failure, since the results returned may in some cases actually match their semantic meanings, rather than redirecting the client to an Escort Service.

Second, B can attempt to access a more specialized cache, which provides information of a range of topics pertinent to Escort Services. Such caches are often provided open-source in high-traffic areas. For example, the author was recently able to obtain "Gentlemen's Guide", "The Space Needle", and "SeXXXy Seattle" on a section of Lake City Way.

Finally, B might access his local router and issue the message {REQ: GOODTIME} to the Cisco (TM) Amusement Button (CAB) driver. CAB drivers are often excellent source of information on Escort Services of all kinds.

Once the identifying information for S has been obtained, B sends an identifying request to S. This request includes a time window and parameters representing the client's servicing wishes. S matches these constraints with its lists of available Hoare's, and returns the matching list along with a monetary metric for each (as in PiMP). Clients then select the Hoare A from the list. Once this exchange of messages has been completed, the client is promised service with in the time window by A or an equivalent or better replacement.

3 Security Considerations

As with all distributed systems, Escort Services are vulnerable to various security exploits and must handle them in a graceful manner. While much recent work has focused on denial-of-service attacks (usually from flash crowds, [4], [5]), and solutions have been shown that scale to several hundred clients, few researchers have looked at the problem of protecting the privacy of the client/service relationship. While many attacks focus on the use of forged client identities, we counterintuitively see this as an opportunity to protect privacy. For example, Bob might forge the identity "John" for the duration of his interaction with the Escort Service and associated Hoare (mean TTLs in the range 0.5 - 1 hour).

4 Future Work

As Escort Services group together and utilize the services of several PiMPs, we might consider leveraging several Escort Services to increase the available stable of Hoares. In the past this has proved tricky; making the respective coordinators work together makes solving distributed consensus look like coding linear search. However, we feel an approach that relies on a hierarchical structure rather than a peer structure may prove feasible. As such, we are currently working on the MasterPiMP system (applications for this position being accepted).

5 Conclusions

We have presented an algorithm for clients to discover Escort Services with a minimum of searching. It is hoped that this work will go further towards enriching the lives of those in 433, many of whom spend a considerable fraction of their gross income trying to get serviced.

References

- [1] R.J. Dunn. Pimp: Rethinking hoare monitors. In *Proceedings of PoCSi433'01*, 2001.
- [2] I.M.A. Hoare. Effective monitoring of hoares. *Fraternal Brotherhood of Panderers Review*, 3847(11), Nov 1987.
- [3] H. Fleiss. Escort services: Experiences in practice. *Fraternal Brotherhood of Panderers Review*, 3853(2), Feb 1993.
- [4] Annabel Chong. *The World's Biggest Gangbang*. Metro Productions, 1995.
- [5] Jasmine St. Claire. *Gang Bang II*. Metro Productions, 1996.